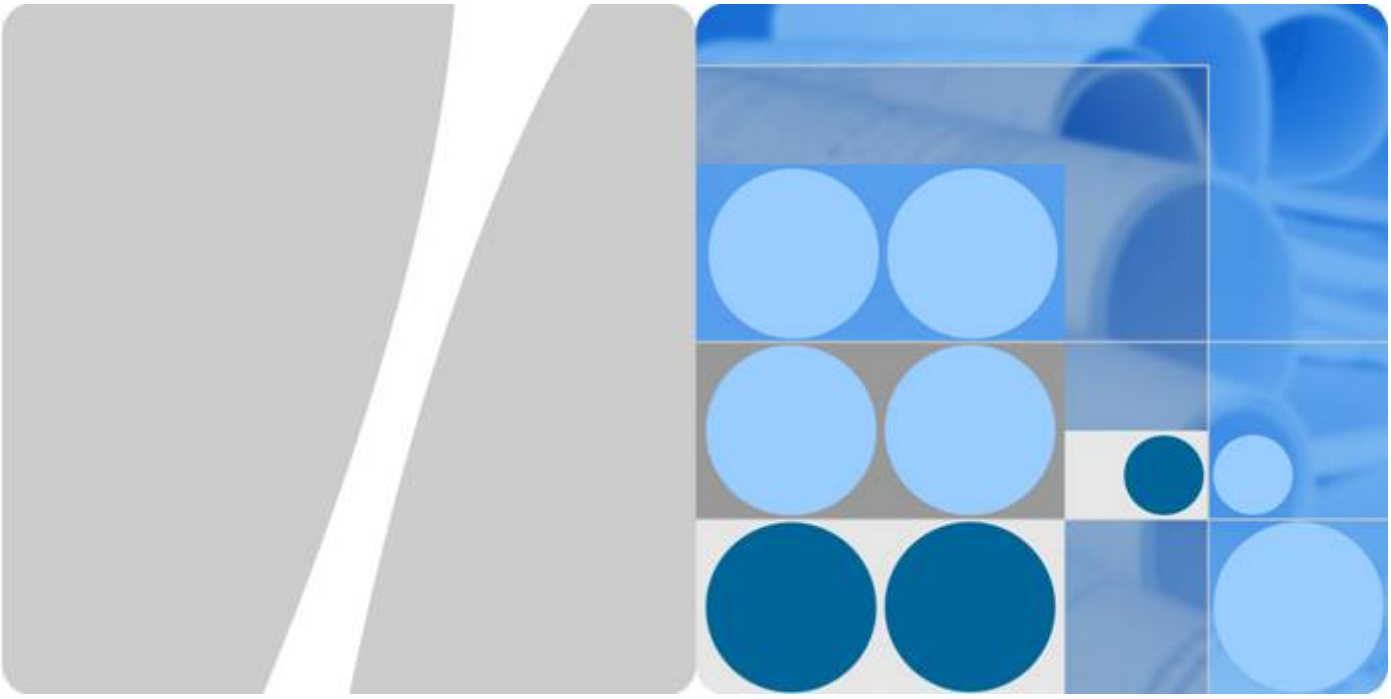


Huawei AR Series Access Routers

V200R010

# CLI-based Configuration Guide - Security


Issue 13

Date 2024-08-30



HUAWEI TECHNOLOGIES CO., LTD.

**Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.**

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

### Trademarks and Permissions


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

### Notice

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

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

## Huawei Technologies Co., Ltd.

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

Website: https://e.huawei.com

# About This Document

## Intended Audience

This document describes the concepts and configuration procedures of security features on the AR, and provides the configuration examples.

This document provides guidance for configuring security features.

This document is intended for:

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

## Symbol Conventions

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

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

 Copyright © Huawei Technologies Co., Ltd. 

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

# Command Conventions

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

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


Copyright © Huawei Technologies Co., Ltd.

# Interface Numbering Conventions

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

# Security Conventions

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

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

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

# Reference Standards and Protocols

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

 Copyright © Huawei Technologies Co., Ltd. 

## Declaration

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

# Mappings Between Product Software Versions and NMS Versions

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

| AR Product Software Version | eSight | iManager U2000 |
| --- | --- | --- |
| V200R010 | V300R009C00 | V200R018C50 |


Copyright © Huawei Technologies Co., Ltd.

# Contents

**About This Document** ii

**1 AAA Configuration** 1

1.1 Overview of AAA 1
1.2 Understanding AAA 2
1.2.1 Domain-based User Management 2
1.2.2 AAA Scheme 7
1.2.2.1 Authentication Scheme 7
1.2.2.2 Authorization Scheme 8
1.2.2.3 Accounting Scheme 11
1.2.3 Local Authentication and Authorization 12
1.2.4 RADIUS AAA 13
1.2.4.1 Overview of RADIUS 13
1.2.4.2 RADIUS Packets 15
1.2.4.3 RADIUS Authentication, Authorization, and Accounting Process 18
1.2.4.4 RADIUS Packet Retransmission Mechanism 19
1.2.4.5 RADIUS Server Selection Mechanism 21
1.2.4.6 RADIUS Server Status Detection 23
1.2.4.7 RADIUS CoA/DM 28
1.2.4.8 RADIUS Attributes 33
1.2.4.9 RADIUS Attribute Disablement and Translation 57
1.2.5 HWTACACS AAA 59
1.2.5.1 Overview of HWTACACS 59
1.2.5.2 HWTACACS Packets 60
1.2.5.3 HWTACACS Authentication, Authorization, and Accounting Process 70
1.2.5.4 HWTACACS Attributes 71
1.2.6 HACA AAA 77
1.2.6.1 Overview of HACA 77
1.2.6.2 HACA Packets 78
1.2.6.3 HACA Authentication, Authorization, and Accounting Process 80
1.3 Application Scenarios for AAA 82
1.4 Licensing Requirements and Limitations for AAA 84
1.5 Default Settings for AAA 85
1.6 Summary of AAA Configuration Tasks 86

 Copyright © Huawei Technologies Co., Ltd. 

1.7 Configuring AAA....87
1.7.1 Configuring Local Authentication and Authorization....87
1.7.1.1 Configuring a Local Server....88
1.7.1.1.1 Configuring a Local User....89
1.7.1.1.2 Configuring Authorization Rules....96
1.7.1.2 Configuring AAA Schemes....98
1.7.1.3 (Optional) Configuring a Service Scheme....100
1.7.1.4 Applying AAA Schemes to a Domain....103
1.7.1.5 Verifying the Local Authentication and Authorization Configuration....105
1.7.2 Using RADIUS to Perform Authentication, Authorization, and Accounting....106
1.7.2.1 Configuring an AAA Scheme....106
1.7.2.2 Configuring a RADIUS Server Template....110
1.7.2.3 (Optional) Configuring the RADIUS Server Status Detection Function....113
1.7.2.4 (Optional) Configuring RADIUS Attributes....114
1.7.2.4.1 Disabling or Translating RADIUS Attributes....115
1.7.2.4.2 Configuring the RADIUS Attribute Check Function....116
1.7.2.4.3 Modifying the Value of a RADIUS Attribute....116
1.7.2.4.4 Configuring Standard RADIUS Attributes....117
1.7.2.4.5 Configuring Huawei Proprietary RADIUS Attributes....118
1.7.2.5 (Optional) Configuring Authorization Information....119
1.7.2.5.1 (Optional) Configuring a Service Scheme....119
1.7.2.5.2 Configuring a User Group....122
1.7.2.6 Creating and Configuring a Domain....123
1.7.2.7 Configuring Global Default Domains....125
1.7.2.8 Applying an AAA Scheme, a RADIUS Server Template, and Authorization Information to a Domain....126
1.7.2.9 Configuring the RADIUS CoA or DM Function....127
1.7.2.10 Verifying the RADIUS AAA Configuration....129
1.7.3 Using HWTACACS to Perform Authentication, Authorization, and Accounting....130
1.7.3.1 Configuring an HWTACACS Server....131
1.7.3.2 Configuring AAA Schemes....131
1.7.3.3 Configuring an HWTACACS Server Template....134
1.7.3.4 (Optional) Configuring a Recording Scheme....139
1.7.3.5 (Optional) Configuring a Service Scheme....140
1.7.3.6 Applying AAA Schemes to a Domain....143
1.7.3.7 Verifying the HWTACACS AAA Configuration....146
1.7.4 Configuring HACA Authentication....146
1.7.4.1 Configuring an HACA Server....147
1.7.4.2 Configuring an AAA Scheme....147
1.7.4.3 Configuring an HACA Server Template....150
1.7.4.4 (Optional) Configuring a Service Scheme....151
1.7.4.5 Applying an AAA Scheme to a Domain....154
1.7.4.6 Verifying the HACA Authentication Configuration....156

 Copyright © Huawei Technologies Co., Ltd. 

1.8 Maintaining AAA 156
1.8.1 Forcing Users to Go Offline 156
1.8.2 Testing Whether a User Can Pass RADIUS Authentication or Accounting 157
1.8.3 Configuring the AAA Alarm Report Function 159
1.8.4 Recording Login and Logout Information 160
1.8.5 Clearing AAA Statistics 161
1.8.6 Clearing HACA Statistics 161
1.9 Configuration Examples for AAA 162
1.9.1 Example for Configuring RADIUS Authentication and Accounting 162
1.9.2 Example for Configuring HWTACACS Authentication, Accounting, and Authorization 166
1.9.3 Example for Configuring Domain-based User Management 170
1.10 FAQ About AAA 176
1.10.1 Why Must the Administrator Pass the AAA Authentication? 176
1.10.2 Why Does RADIUS Authentication Fail When the RADIUS Server Template and RADIUS Server Are Properly Configured? 176
1.10.3 Why Does the Server Checking Error Occur During RADIUS Dynamic Authentication? 177
1.10.4 Why Does HWTACACS Authentication Fail When the HWTACACS Server Template and HWTACACS Server Are Properly Configured? 177
1.10.5 Why Are Accounting Packets Received When Commands Are Run on Devices? 177
1.10.6 Why Are the 802.1x Users' IP Addresses Not Displayed After I Run the Display Access-User Command? 177
1.10.7 Which Attributes Are Required by ACLs Dynamically Delivered by the RADIUS Server? 177
1.10.8 Which Attributes Are Required by VLANs Dynamically Delivered by the RADIUS Server? 178
1.10.9 What Are the Restrictions on Using HWTACACS? 178
1.10.10 Does the Router Support User Level Settings Using RADIUS? How Can I Configure It? 178
1.10.11 Level 1 Is Configured for a User on the RADIUS Server, But the User Has More Rights Than Rights Defined in Level 1 After Login. Why? 178
1.10.12 How Do I Convert RADIUS Attributes After Replacing an ME60 Gateway with an AR Router? 178

**2 DAA Configuration 180**

2.1 Overview of DAA 180
2.2 Understanding DAA 181
2.3 Application Scenarios for DAA 182
2.4 Summary of DAA Configuration Tasks 183
2.5 Licensing Requirements and Limitations for DAA 185
2.6 Default Settings for DAA 185
2.7 Configuring DAA 186
2.7.1 Configuring Traffic Identification Rules 186
2.7.2 Configuring the Tariff Level 187
2.7.3 Configuring Traffic-based Accounting 188
2.7.4 Verifying the DAA Configuration 189
2.8 Configuration Examples for DAA 190
2.8.1 Example for Configuring Accounting for the Specified Network 190

**3 NAC Configuration 195**

 Copyright © Huawei Technologies Co., Ltd. 

3.1 Overview of NAC 195
3.2 Understanding NAC 197
3.2.1 NAC Fundamentals 197
3.2.2 802.1X Authentication 199
3.2.3 MAC Address Authentication 202
3.2.4 Portal Authentication 204
3.3 Application Scenarios for NAC 207
3.4 Licensing Requirements and Limitations for NAC 209
3.5 Default Settings for NAC 210
3.6 Configuring NAC 212
3.6.1 Configuration Procedure for NAC 212
3.6.2 Configuring an Access Profile 214
3.6.2.1 Configuring an 802.1X Access Profile 214
3.6.2.1.1 Creating an 802.1X Access Profile 214
3.6.2.1.2 (Optional) Configuring an Authentication Mode for 802.1X Users 214
3.6.2.1.3 (Optional) Configuring the Packet Types That Can Trigger 802.1X Authentication 216
3.6.2.1.4 (Optional) Configuring the Authorization State of an Interface 216
3.6.2.1.5 (Optional) Configuring the Device to Send EAP Packets with a Code Number to 802.1X Users 217
3.6.2.1.6 (Optional) Configuring Re-authentication for Online 802.1X Authentication Users 218
3.6.2.1.7 (Optional) Configuring the Online User Handshake Function 219
3.6.2.1.8 (Optional) Configuring Network Access Rights for Users When the 802.1X Client Does Not Respond 220
3.6.2.1.9 (Optional) Configuring the Device to Automatically Generate the DHCP Snooping Binding Table for Static IP Users 221
3.6.2.1.10 (Optional) Configuring the Number of Times an Authentication Request or Handshake Packet Is Retransmitted to an 802.1X User 223
3.6.2.1.11 (Optional) Configuring the Authentication Timeout Timer for 802.1X Clients 223
3.6.2.1.12 (Optional) Configuring the Function of Triggering 802.1X Authentication Through Multicast Packets 224
3.6.2.1.13 (Optional) Configuring MAC Address-based Dynamic VLAN Assignment 225
3.6.2.1.14 Verifying the 802.1X Access Profile Configuration 226
3.6.2.2 Configuring a MAC Access Profile 226
3.6.2.2.1 Creating a MAC Access Profile 226
3.6.2.2.2 (Optional) Configuring the Authentication Mode for MAC Address Authentication 227
3.6.2.2.3 Configuring the User Name Format for MAC Address Authentication 227
3.6.2.2.4 (Optional) Configuring Packet Types That Can Trigger MAC Address Authentication 228
3.6.2.2.5 (Optional) Configuring a Source MAC Address Segment Allowed by MAC Address Authentication 229
3.6.2.2.6 (Optional) Configuring Re-authentication for Online MAC Address Authentication Users 230
3.6.2.2.7 (Optional) Configuring the Device to Automatically Generate the DHCP Snooping Binding Table for Static IP Users 231
3.6.2.2.8 (Optional) Configuring MAC Address-based Dynamic VLAN Assignment 233
3.6.2.2.9 Verifying the MAC Access Profile Configuration 233

 Copyright © Huawei Technologies Co., Ltd. 

3.6.3 Configuring an Authentication Profile....233
3.6.3.1 Creating an Authentication Profile....234
3.6.3.2 Configuring a User Authentication Mode....234
3.6.3.3 (Optional) Configuring the User Access Mode....236
3.6.3.4 (Optional) Configuring Authentication Event Authorization Information....237
3.6.3.5 (Optional) Configuring Authentication-Free Authorization Information....240
3.6.3.5.1 (Optional) Configuring Authorization Information for Authentication-free Users....240
3.6.3.6 (Optional) Configuring Re-authentication for Users....241
3.6.3.7 (Optional) Configuring the Handshake Function to Enable the Device to Clear User Entries Immediately....242
3.6.3.8 (Optional) Configuring a User Authentication Domain....243
3.6.3.9 (Optional) Configuring the User Logout Delay Function When an Interface Link Is Faulty....244
3.6.3.10 (Optional) Reauthenticating users When the Time Exceeds the Value of Session-Timeout....245
3.6.3.11 Verifying the Authentication Profile Configuration....246
3.6.4 NAC Application....246
3.6.5 (Optional) Configuring NAC Extended Functions....248
3.6.5.1 Configuring Extended Functions Related to 802.1X Authentication....248
3.6.5.1.1 Configuring the Interval for Sending 802.1X Authentication Requests....248
3.6.5.1.2 Configuring 802.1X-based Fast Deployment....249
3.6.5.2 Configuring Extended Functions Related to Portal Authentication....250
3.6.5.2.1 Configuring CNA Bypass for iOS Terminals....250
3.6.5.2.2 Configuring the CNA Adaptive Function for iOS Terminals....250
3.6.5.2.3 Configuring the Maximum Number of Portal Authentication Users Allowed on the Device....251
3.6.5.2.4 (Optional) Forcing Portal Authentication Users Offline When a 3G/LTE Link Is Disconnected....252
3.6.5.3 Configuring the Quiet Function....253
3.6.5.4 Configuring the Web Push Function....254
3.6.5.5 (Optional) Configuring HTTP-based Authentication and Accounting Functions....256
3.6.5.6 Configuring the Maximum Number of Consecutive Authentication Failures....258
3.6.5.7 Adjusting the Matching Order of ACL Rules....258
3.6.5.8 Configuring User Isolation....258
3.6.5.9 Setting the Source Address of Offline Detection Packets....259
3.6.5.10 Enabling the Device to Dynamically Adjust the Rate at Which It Processes Packets from NAC Users....260
3.6.5.11 Enabling URL Encoding and Decoding....260
3.6.5.12 Verifying the NAC Extended Functions Configuration....261
3.7 Maintaining NAC....261
3.7.1 Configuring the NAC Alarm Report Function....261
3.7.2 Clearing NAC Statistics....262
3.7.3 Monitoring NAC Operation....262
3.8 Configuration Examples for NAC....263
3.8.1 Example for Configuring 802.1X Authentication....263
3.8.2 Example for Configuring MAC Address Authentication....267
3.8.3 Example for Configuring Layer 2 External Portal Authentication....270

 Copyright © Huawei Technologies Co., Ltd. 

3.8.4 Example for Configuring Layer 3 External Portal Authentication....275
3.9 FAQ....281
3.9.1 When Does the 802.1x Dynamic VLAN Take Effect?....281
3.9.2 Why Are the 802.1x Users' IP Addresses Not Displayed After I Run the Display Access-User Command?....281
3.9.3 Which Domain Is Preferentially Used to Authenticate Users in mac-authen Mode?....281
3.9.4 Which Domain Is Used Preferentially by 802.1x Users?....281
3.9.5 What Are the Functions of the Domain Configured on a WLAN-BSS Interface?....281
3.9.6 Can MAC Bypass Authentication Be Configured on a Fixed Port on the SRU?....282
**4 Terminal Access Configuration....283**
4.1 Overview of BRAS Access....283
4.2 Configuring Terminal Access....284
4.3 Configuration Examples for BRAS Access....288
4.3.1 Example for Configuring Terminal access in Which Portal Authentication Is Used....288
4.3.2 Example for Configuring Terminal access in Which PPPoE Authentication Is Used....293
**5 ACL Configuration....299**
5.1 Overview of ACLs....299
5.2 Understanding ACLs....301
5.2.1 ACL Fundamentals....301
5.2.2 ACL Classification....304
5.2.3 Step....305
5.2.4 Matching Order....307
5.2.5 Matching Conditions....310
5.2.6 Time Range....320
5.2.7 Default ACL Actions and Mechanisms of Different Service Modules....321
5.2.8 ACL Configuration Guidelines....329
5.3 Application Scenarios for ACLs....332
5.3.1 Using an ACL to Control Telnet Login Rights....332
5.3.2 Applying an ACL to SNMP to Filter NMSs....332
5.3.3 Using an ACL to Restrict Mutual Access Between Network Segments....333
5.3.4 Using an ACL to Prevent Certain Users from Accessing the Internet in the Specified Time Range....334
5.3.5 Using an ACL in QoS to Implement Traffic Policing....335
5.3.6 Using an ACL to Filter OSPF Routes....335
5.3.7 Using ACL in NAT to Filter Traffic....336
5.3.8 Applying ACLs to the Firewall....337
5.4 Summary of ACL Configuration Tasks....338
5.5 Licensing Requirements and Limitations for ACLs....340
5.6 Default Settings for ACLs....340
5.7 Configuring ACLs....341
5.7.1 Configuring and Applying a Basic ACL....341
5.7.1.1 (Optional) Creating a Time Range in Which an ACL Takes Effect....341
5.7.1.2 (Optional) Configuring the Port Set....342

 Copyright © Huawei Technologies Co., Ltd. 

5.7.1.3 Configuring a Basic ACL ..... 343
5.7.1.4 Applying a Basic ACL ..... 345
5.7.1.5 Verifying a Basic ACL Configuration ..... 350
5.7.2 Configuring and Applying an Advanced ACL ..... 350
5.7.2.1 (Optional) Creating a Time Range in Which an ACL Takes Effect ..... 350
5.7.2.2 Configuring an Advanced ACL ..... 350
5.7.2.3 Applying an Advanced ACL ..... 354
5.7.2.4 Verifying an Advanced ACL Configuration ..... 356
5.7.3 Configuring and Applying a Layer 2 ACL ..... 356
5.7.3.1 (Optional) Creating a Time Range in Which an ACL Takes Effect ..... 357
5.7.3.2 Configuring a Layer 2 ACL ..... 357
5.7.3.3 Applying a Layer 2 ACL ..... 359
5.7.3.4 Verifying a Layer 2 ACL Configuration ..... 361
5.7.4 Configuring and Applying a User ACL ..... 361
5.7.4.1 (Optional) Creating a Time Range in Which an ACL Takes Effect ..... 361
5.7.4.2 Configuring a User ACL ..... 361
5.7.4.3 Applying a User ACL ..... 363
5.7.4.4 Verifying a User ACL Configuration ..... 364
5.7.5 Configuring and Applying a Basic ACL6 ..... 364
5.7.5.1 (Optional) Creating a Time Range in Which an ACL6 Takes Effect ..... 364
5.7.5.2 Configuring a Basic ACL6 ..... 364
5.7.5.3 Applying a Basic ACL6 ..... 366
5.7.5.4 Verifying a Basic ACL6 Configuration ..... 369
5.7.6 Configuring and Applying an Advanced ACL6 ..... 370
5.7.6.1 (Optional) Creating a Time Range in Which an ACL6 Takes Effect ..... 370
5.7.6.2 Configuring an Advanced ACL6 ..... 370
5.7.6.3 Applying an Advanced ACL6 ..... 373
5.7.6.4 Verifying an Advanced ACL6 Configuration ..... 375
5.8 Maintaining ACLs ..... 376
5.8.1 Adjusting the Step of ACL Rules ..... 376
5.8.2 Displaying ACL Resources ..... 376
5.8.3 Optimizing ACL Resources ..... 377
5.8.4 Clearing ACL Statistics ..... 378
5.9 Configuration Examples for ACLs ..... 378
5.9.1 Example for Using Basic ACLs to Restrict FTP Access Rights ..... 378
5.9.2 Example for Using Basic ACLs to Control Telnet Login Rights ..... 380
5.9.3 Example for Applying Basic ACLs to SNMP to Filter NMSs ..... 382
5.9.4 Example for Using Basic ACLs to Filter OSPF Routes ..... 386
5.9.5 Example for Configuring a Basic ACL in URPF to Prevent Source IP Address Spoofing Attacks ..... 390
5.9.6 Example for Using Advanced ACLs to Restrict Mutual Access Between Network Segments ..... 392
5.9.7 Example for Using Advanced ACLs to Control Access to the Specified Server in the Specified Time Range ..... 396
5.9.8 Example for Using an Advanced ACL to Configure the Firewall Function ..... 400

 Copyright © Huawei Technologies Co., Ltd. 

5.9.9 Example for Using Layer 2 ACLs to Block Network Access of the Specified Users....403
5.9.10 Example for Using Layer 2 ACLs in QoS to Implement Traffic Policing....406
5.9.11 Example for Using Advanced ACL6s to Filter Certain Types of IPv6 Packets....410
5.10 Troubleshooting ACLs....412
5.10.1 Services Are Interrupted Due to Incorrect IP Address Wildcard Mask....412
5.10.2 Users Cannot Access the Internet Because the DNS Server Address Is Blocked....413
5.10.3 Time Range-based ACL Does Not Take Effect Due to Incorrect System Time....414
5.11 FAQ About ACLs....415
5.11.1 In Which Methods Can ACLs Be Delivered?....415
5.11.2 What Is the Relationship Between the permit/deny Rules in an ACL and Those in the Behavior of a Traffic Policy?....419
5.11.3 How Can I Check the Order in Which ACL Rules Take Effect?....419
5.11.4 How Can Unidirectional Access Control Be Implemented?....420
5.11.5 Which Packets Cannot Be Filtered by the ACL Used by a Traffic Policy?....422
5.11.6 How Are deny and permit Actions in ACL Rules Used in Different Services?....422

**6 Firewall Configuration....426**

6.1 Overview of Firewalls....427
6.2 Understanding Firewalls....427
6.2.1 Security Zone and Interzone....427
6.2.2 Firewall Working Mode....428
6.2.3 Packet Filtering Firewall....429
6.2.4 Stateful Firewall....429
6.2.5 Blacklist....432
6.2.6 Whitelist....433
6.2.7 Port Mapping....434
6.2.8 Attack Defense....434
6.2.9 Traffic Statistics Collection and Monitoring....443
6.2.10 Firewall Log....444
6.2.11 Virtual Firewall....445
6.2.12 Firewall in HSB Mode....445
6.3 Application Scenarios for Firewalls....448
6.3.1 Firewall Between the Internal and External Networks....448
6.3.2 Firewall on an Internal Network....448
6.4 Licensing Requirements and Limitations for Firewalls....449
6.5 Default Settings for Firewalls....449
6.6 Configuring Basic Functions of the Firewall....451
6.6.1 Creating a Zone and Adding Interfaces to the Zone....451
6.6.2 Creating an Interzone....452
6.6.3 Enabling Firewall in an Interzone....452
6.6.4 (Optional) Configuring the Aging Time of the Firewall Session Table....453
6.6.5 Verifying the Basic Firewall Functions Configuration....454
6.7 Configuring the Packet Filtering Firewall....454

 Copyright © Huawei Technologies Co., Ltd. 

6.7.1 (Optional) Configuring the Default Processing Mode for Unmatched Packets....454
6.7.2 Configuring ACL-based Packet Filtering in an Interzone....455
6.7.3 Verifying the Packet Filtering Firewall Configuration....457
6.8 Configuring Stateful Firewall (ASPF)....457
6.9 Configuring the Blacklist....458
6.9.1 Enabling the Blacklist Function....458
6.9.2 Configuring a Blacklist Entry....459
6.9.3 Configuring Blacklist or Whitelist Entries in Batches....460
6.9.4 Verifying the Blacklist Configuration....461
6.10 Configuring the Whitelist....461
6.10.1 Configuring a Whitelist Entry....461
6.10.2 Configuring Blacklist or Whitelist Entries in Batches....462
6.10.3 Verifying the Whitelist Configuration....463
6.11 Configuring Port Mapping....463
6.12 Configuring Attack Defense....464
6.12.1 Enabling the Attack Defense Function....464
6.12.2 Setting the Parameters for Flood Attack Defense....465
6.12.3 Configuring Large ICMP Packet Attack Defense....466
6.12.4 Setting Parameters for Scanning Attack Defense....466
6.12.5 Verifying the Attack Defense Configuration....467
6.13 Configuring Traffic Statistics and Monitoring....467
6.13.1 Setting the Session Thresholds for System-Level Traffic Statistics and Monitoring....467
6.13.2 Setting the Session Thresholds for Zone-Level Traffic Statistics and Monitoring....468
6.13.3 Setting the Session Thresholds for IP Address-Level Traffic Statistics and Monitoring....469
6.13.4 Verifying the Traffic Statistics and Monitoring Configuration....470
6.14 Configuring the Firewall Log Function....470
6.15 Configuring Virtual Firewalls....471
6.15.1 Configuring a VPN Instance to Identify a Virtual Firewall....471
6.15.2 Configuring Security Functions for a Virtual Firewall....472
6.15.3 Verifying the Virtual Firewall Configuration....474
6.16 Configuring Firewalls in HSB Mode....474
6.16.1 Configuring an HSB Service....474
6.16.2 Configuring an HSB Group....476
6.16.3 Enabling an HSB Group....477
6.16.4 Verifying the HSB Configuration....477
6.17 Maintaining the Firewall....477
6.17.1 Displaying the Firewall Configuration....477
6.17.2 Clearing the Firewall Statistics....479
6.17.3 Clearing Statistics on Firewall Application Entries....479
6.17.4 Clearing Attack Defense Statistics on Firewall....479
6.18 Configuration Examples for Firewalls....480
6.18.1 Example for Configuring the ACL-based Packet Filtering Firewall....480

 Copyright © Huawei Technologies Co., Ltd. 

6.18.2 Example for Configuring ASPF and Port Mapping....482
6.18.3 Example for Configuring the Blacklist....485
6.18.4 Example for Configuring Blacklists on Virtual Firewalls....488
6.18.5 Example for Configuring Firewall HSB....491
6.19 FAQ About Firewalls....497
6.19.1 How Do I Delete and View the Firewall and NAT Flow Table?....497
6.19.2 How Can I View the ACL Hit Count Configured on the Packet Filtering Firewall?....497
6.19.3 Which Protocols Does the AR Firewall ASPF Support?....497
6.19.4 What Are the Types of Blacklists? (Firewall)....497
**7 Deep Security Defense Configuration....498**
7.1 Security Policy....498
7.1.1 Overview of Security Policies....498
7.1.2 Understanding Security Policies....499
7.1.3 Application Scenarios for Security Policies....503
7.2 IPS Configuration....504
7.2.1 Overview of IPS....504
7.2.2 Understanding IPS....506
7.2.3 Application Scenarios for IPS....510
7.2.3.1 Using IPS to Block Intrusion Behaviors....510
7.2.4 Licensing Requirements and Limitations for IPS....511
7.2.5 Default Settings for IPS....512
7.2.6 Enabling the Deep Security Function....514
7.2.7 Updating the IPS Signature Database....515
7.2.8 Configuring IPS....519
7.2.8.1 (Optional) Configuring User-Defined Signatures....519
7.2.8.2 Configuring IPS Profiles....521
7.2.8.3 Binding an IPS Profile to a Security Policy....526
7.2.8.4 Applying a Security Policy in Interzones....527
7.2.8.5 (Optional) Controlling the IPS Log Sending Function....528
7.2.8.6 Verifying the IPS Configuration....529
7.2.9 Maintaining IPS....530
7.2.9.1 Viewing IPS Statistics....530
7.2.9.2 Clearing IPS Statistics....530
7.2.10 Configuration Examples for IPS....531
7.2.10.1 Example for Configuring IPS to Block Intrusion Behaviors....531
7.3 URL Filtering Configuration....535
7.3.1 Overview of URL Filtering....536
7.3.2 Understanding URL Filtering....536
7.3.2.1 URL Matching Mode....536
7.3.2.2 Working Mechanism of URL Filtering....539
7.3.3 Applicable Scenarios for URL Filtering....542
7.3.3.1 Using URL Filtering to Regulate Online Behaviors....542

 Copyright © Huawei Technologies Co., Ltd. 

7.3.4 Licensing Requirements and Limitations for URL Filtering 543
7.3.5 Enabling the Deep Security Function 545
7.3.6 Configuring URL Filtering 545
7.3.6.1 Configuring a URL Filtering Profile 545
7.3.6.2 Binding a URL Filtering Profile to a Security Policy 550
7.3.6.3 Binding the Security Policy to an Interzone 551
7.3.6.4 (Optional) Configuring the Device to Control generating of URL Filtering Logs 552
7.3.6.5 (Optional) Configuring user group-based URL Filtering 553
7.3.6.6 Verifying the URL Filtering Configuration 553
7.3.7 Maintaining URL Filtering 554
7.3.7.1 Displaying URL Filtering Statistics 554
7.3.7.2 Clearing URL Filtering Statistics 554
7.3.8 Configuration Examples for URL Filtering 555
7.3.8.1 Example for Configuring URL Filtering to Regulate Online Behaviors of Employees 555
**8 Local Attack Defense Configuration 560**
8.1 Overview of Local Attack Defense 560
8.2 Licensing Requirements and Limitations for Local Attack Defense 562
8.3 Default Settings for Local Attack Defense 562
8.4 Configuring CPU Attack Defense 564
8.4.1 Creating an Attack Defense Policy 565
8.4.2 Configuring a Blacklist 565
8.4.3 Configuring Dynamic CPCAR Adjustment 566
8.4.4 Configuring the Rate Limit for Packets Sent to the CPU 567
8.4.5 Setting the Priority for Packets of a Specified Protocol 567
8.4.6 Configuring ALP 568
8.4.7 Configuring the Rate Limit for All Packets Sent to the CPU 569
8.4.8 Applying an Attack Defense Policy 570
8.4.9 Verifying the CPU Attack Defense Configuration 570
8.5 Configuring Attack Source Tracing 570
8.5.1 Creating an Attack Defense Policy 571
8.5.2 Configuring the Threshold for Attack Source Tracing 571
8.5.3 Configuring an Attack Source Tracing Mode 572
8.5.4 Configuring the Types of Traced Packets 573
8.5.5 Configuring Event Reporting Function 573
8.5.6 Configuring Attack Source Punish Actions 574
8.5.7 Applying an Attack Defense Policy 575
8.5.8 Verifying the Attack Source Tracing Configuration 575
8.6 Maintaining Local Attack Defense 575
8.6.1 Clearing Attack Source Information 575
8.6.2 Clearing Statistics About Packets Sent to the CPU 576
8.7 Configuration Examples for Local Attack Defense 576
8.7.1 Example for Configuring Local Attack Defense 576

 Copyright © Huawei Technologies Co., Ltd. 

8.8 Troubleshooting Local Attack Defense....580
8.8.1 Attack Source Tracing Does Not Take Effect....580
8.8.2 The Blacklist Does Not Take Effect....581
8.9 FAQ About Local Attack Defense....581
8.9.1 What Can I Do with Excess ACL Rules Used by a Blacklist in Local Attack Defense?....581
8.9.2 How Do I Configure CPCAR?....581
8.9.3 Why Does the CPCAR Rate Limit Configuration Not Take Effect?....582
**9 Attack Defense Configuration....583**
9.1 Overview of Attack Defense....583
9.2 Understanding Attack Defense....584
9.2.1 Defense Against Malformed Packet Attacks....584
9.2.2 Defense Against Packet Fragment Attacks....585
9.2.3 Defense Against Flood Attacks....591
9.3 Application Scenarios for Attack Defense....592
9.4 Licensing Requirements and Limitations for Attack Defense....593
9.5 Default Settings for Attack Defense....593
9.6 Configuring Defense Against Malformed Packet Attacks....594
9.7 Configuring Defense Against Packet Fragment Attacks....594
9.8 Configuring Defense Against Flood Attacks....595
9.8.1 Configuring Defense Against TCP SYN Flood Attacks....595
9.8.2 Configuring Defense Against UDP Flood Attacks....596
9.8.3 Configuring Defense Against ICMP Flood Attacks....596
9.8.4 Verifying the Flood Attack Defense Configuration....597
9.9 Clearing Attack Defense Statistics....597
9.10 Configuration Examples for Attack Defense....598
9.10.1 Example for Configuring Attack Defense....598
**10 Traffic Suppression Configuration....600**
10.1 Overview of Traffic Suppression....600
10.2 Understanding Traffic Suppression....601
10.2.1 Traffic Suppression....601
10.3 Application Scenarios for Traffic Suppression....601
10.3.1 Traffic Suppression....601
10.4 Licensing Requirements and Limitations for Traffic Suppression....602
10.5 Default Settings for Traffic Suppression....602
10.6 Configuring Traffic Suppression....602
10.6.1 Configuring Traffic Suppression on an Interface....602
10.6.2 Limiting the Rate of ICMP Packets....603
10.6.3 Verifying the Traffic Suppression Configuration....604
10.7 Configuration Examples for Traffic Suppression....605
10.7.1 Example for Setting the Rate Limit in pps for Traffic Suppression....605
10.8 Troubleshooting Traffic Suppression....606
10.8.1 Broadcast Traffic Suppression Does Not Take Effect....606

 Copyright © Huawei Technologies Co., Ltd. 

10.9 FAQ About Traffic Suppression 607
10.9.1 Why Is the Actual Suppression Value Different from the Configured Traffic Suppression Value? 607
**11 ARP Security Configuration 609**
11.1 Overview of ARP Security 609
11.2 Understanding ARP Security 613
11.2.1 Rate Limiting on ARP Packets 613
11.2.2 Rate Limiting on ARP Miss Messages 614
11.2.3 Strict ARP Learning 616
11.2.4 ARP Entry Limiting 617
11.2.5 ARP Entry Fixing 617
11.2.6 DAI 619
11.2.7 ARP Gateway Anti-Collision 621
11.2.8 Gratuitous ARP Packet Sending 622
11.2.9 MAC Address Consistency Check in an ARP Packet 623
11.2.10 ARP Packet Validity Check 623
11.2.11 ARP Learning Triggered by DHCP 624
11.3 Application Scenarios for ARP Security 624
11.3.1 Defense Against ARP Flood Attacks 624
11.3.2 Defense Against ARP Spoofing Attacks 626
11.4 Licensing Requirements and Limitations for ARP Security 627
11.5 Default Settings for ARP Security 627
11.6 Configuring ARP Security 628
11.6.1 Configuring Defense Against ARP Flood Attacks 629
11.6.1.1 Configuring Rate Limiting on ARP Packets based on Source MAC Addresses 629
11.6.1.2 Configuring Rate Limiting on ARP Packets based on Source IP Addresses 630
11.6.1.3 Configuring Rate Limiting on ARP Packets Globally or on an Interface 630
11.6.1.4 Configuring Rate Limiting on ARP Packets on the VLANIF Interface of a Super-VLAN 632
11.6.1.5 Configuring Rate Limiting on ARP Miss Messages based on Source IP Addresses 633
11.6.1.6 Configuring Rate Limiting on ARP Miss Messages Globally 634
11.6.1.7 Configuring the Aging Time of Temporary ARP Entries 635
11.6.1.8 Configuring Strict ARP Learning 635
11.6.1.9 Configuring Interface-based ARP Entry Limiting 637
11.6.1.10 Verifying the ARP Flood Attack Defense Configuration 638
11.6.2 Configuring Defense Against ARP Spoofing Attacks 638
11.6.2.1 Configuring ARP Entry Fixing 639
11.6.2.2 Configuring DAI 639
11.6.2.3 Configuring ARP Gateway Anti-Collision 641
11.6.2.4 Configuring Gratuitous ARP Packet Sending 642
11.6.2.5 Configuring MAC Address Consistency Check in an ARP Packet 643
11.6.2.6 Configuring ARP Packet Validity Check 644
11.6.2.7 Configuring Strict ARP Learning 644
11.6.2.8 Configuring ARP Learning Triggered by DHCP 646

 Copyright © Huawei Technologies Co., Ltd. 

11.6.2.9 Verifying the ARP Spoofing Attack Defense Configuration....646
11.7 Maintaining ARP Security....647
11.7.1 Monitoring ARP Running Status....647
11.7.2 Clearing ARP Security Statistics....647
11.7.3 Configuring the Alarm Function for Potential ARP Attacks....648
11.8 Configuration Examples for ARP Security....648
11.8.1 Example for Configuring ARP Security Functions....648
11.8.2 Example for Configuring Defense Against ARP MITM Attacks (All Product Models Except AR100&AR120&AR150&AR160&AR200&AR1200)....653
11.9 FAQ About ARP Security....655
11.9.1 After I Enable ARP Gateway Anti-Collision, and Send Gateway Collision ARP Packets from a MAC Address, Why Can the MAC Address Not Forward Traffic?....656
11.9.2 After I Send ARP Request Packets with the Same Source IP Address, Why Do I Sometimes Receive Response Packets Only at the Rate of 5 Packets Per Second?....656
11.9.3 How Do I Take Measures to Prevent Internal Network Attacks?....656

**12 Port Security Configuration....657**

12.1 Overview of Port Security....657
12.2 Understanding Port Security....657
12.3 Application Scenarios for Port Security....659
12.4 Licensing Requirements and Limitations for Port Security....660
12.5 Default Settings for Port Security....661
12.6 Configuring Port Security....661
12.6.1 Configuring the Secure MAC Address Function....662
12.6.2 Configuring the Sticky MAC Address Function....663
12.7 Configuration Examples for Port Security....665
12.7.1 Example for Configuring Port Security....665

**13 DHCP Snooping Configuration....668**

13.1 Overview of DHCP Snooping....668
13.2 Understanding DHCP Snooping....669
13.2.1 DHCP Snooping Fundamentals....669
13.2.2 Option 82 Supported by DHCP Snooping....670
13.2.3 LDRA Supported by DHCPv6 Snooping....671
13.2.4 Option 18 and Option 37 Fields Supported by DHCPv6 Snooping....672
13.3 Application Scenarios for DHCP Snooping....672
13.3.1 Defense Against Bogus DHCP Server Attacks....673
13.3.2 Defense Against Bogus DHCP Message Attacks....674
13.3.3 Defense Against DHCP Server DoS Attacks....674
13.3.4 Typical Application of the Option 82 Field....675
13.3.5 Detecting Client Locations Through an LDRA....676
13.4 Licensing Requirements and Limitations for DHCP Snooping....677
13.5 Default Settings for DHCP Snooping....678
13.6 Configuring Basic Functions of DHCP Snooping....678

 Copyright © Huawei Technologies Co., Ltd. 

13.6.1 Enabling DHCP Snooping 679
13.6.2 Configuring an Interface as a Trusted Interface 680
13.6.3 (Optional) Enabling Location Transition for DHCP Snooping Users 681
13.6.4 (Optional) Configuring Association Between ARP and DHCP Snooping 681
13.6.5 (Optional) Configuring the Device to Discard DHCP Request Messages When GIADDR Field Is Not 0 682
13.6.6 (Optional) Disabling DHCP Snooping on an Interface 683
13.6.7 Verifying the DHCP Snooping Configuration 683
13.7 Configuring DHCP Snooping Attack Mitigation 684
13.7.1 Configuring Defense Against Bogus DHCP Server Attacks 684
13.7.2 Configuring Defense Against Bogus DHCP Message Attacks 685
13.7.3 Configuring Defense Against DHCP Server DoS Attacks 686
13.7.4 Verifying the DHCP Snooping Attack Defense Configuration 688
13.8 Inserting the Option 82 Field in a DHCP Message 689
13.9 Configuring the LDRA to Detect Client Locations 691
13.10 Inserting the Option 18 or Option 37 Field in a DHCPv6 Message 693
13.11 Maintaining DHCP Snooping 695
13.11.1 Clearing DHCP Snooping Statistics 695
13.11.2 Clearing DHCP Snooping Binding Entries 695
13.11.3 Backing Up DHCP Snooping Binding Entries 696
13.12 Configuration Examples for DHCP Snooping 696
13.12.1 Example for Configuring DHCP Snooping Attack Defense 696
13.12.2 Example for Configuring LDRA to Detect Client Locations 700
13.13 Troubleshooting DHCP Snooping 703
13.13.1 DHCP Clients Cannot Go Online Due to DHCP Snooping 703
13.14 FAQ About DHCP Snooping 704
13.14.1 Can a Router Provide DHCP Snooping Function Without Using a LAN Card? 704

**14 IPSG Configuration 705**

14.1 Overview of IPSG 705
14.2 Understanding IPSG 706
14.2.1 IPSG Fundamentals 706
14.2.2 IPSG Deployment 710
14.2.3 Comparison Between IPSG and Other Features 711
14.3 Application Scenarios for IPSG 716
14.4 Licensing Requirements and Limitations for IPSG 718
14.5 Default Settings for IPSG 718
14.6 Configuring IPSG 718
14.6.1 Configuring IPSG Based on a Static Binding Table 719
14.6.2 Configuring IPSG Based on a Dynamic Binding Table 721
14.7 Configuration Examples for IPSG 724
14.7.1 Example for Configuring IPSG Based on the Static Binding Table to Prevent Host to Use the IP Address of Another Host without Permission 724

 Copyright © Huawei Technologies Co., Ltd. 

14.7.2 Example for Configuring IPSG Based on the DHCP Snooping Dynamic Binding Table to Prevent Host to Use the IP Address of Another Host without Permission 726
14.7.3 Example for Configuring IPSG Based on the Static Binding Table to Prevent Unauthorized Hosts from Accessing the intranet 729
14.8 Troubleshooting IPSG 732
14.8.1 IPSG Does Not Take Effect Because IPSG Is Not Enabled on the Interface or VLAN 732
14.8.2 An Authorized Host Cannot Go Online Due to the Incorrect Static Binding Entry 733
14.8.3 Service Is Abnormal Because the Upstream Interface Is Not Configured as a Trusted Interface 734
14.8.4 Service Is Interrupted After IPSG Is Enabled on the Upstream Interface 735
14.8.5 Unbound Hosts Can Go Online After IP and MAC Bindings Are Configured 736
14.8.6 IPSG Does Not Take Effect When Dynamic IP Address Allocation Is Used Because DHCP Snooping Is Not Configured 737
14.9 FAQ About IPSG 738
14.9.1 Does a Router Support the Binding of One Interface and Multiple IP Addresses 738
14.9.2 Does a Router Support the Binding of One MAC Address and Multiple IP Addresses 738
14.9.3 Which Router Models Support IPSG 739
**15 URPF Configuration 740**
15.1 Overview of URPF 740
15.2 Understanding URPF 741
15.3 Application Scenarios for URPF 742
15.4 Licensing Requirements and Limitations for URPF 744
15.5 Default Settings for URPF 744
15.6 Configuring URPF 744
15.6.1 Configuring the URPF Check Mode on an Interface 744
15.6.2 Verifying the URPF Configuration 745
15.7 Configuration Examples for URPF 746
15.7.1 Example for Configuring URPF 746
**16 PKI Configuration 748**
16.1 Overview of PKI 748
16.2 Understanding PKI 749
16.2.1 Basic Concepts of PKI 749
16.2.1.1 Cryptography 750
16.2.1.2 Digital Envelope and Digital Signature 752
16.2.1.3 Digital Certificate 755
16.2.2 PKI System Structure 758
16.2.3 PKI Working Mechanism 762
16.3 Application Scenarios for PKI 764
16.3.1 PKI Application in IPSec VPN 764
16.4 Licensing Requirements and Limitations for PKI 765
16.5 Default Settings for PKI 766
16.6 Summary of PKI Configuration Tasks 766
16.7 Configuring PKI 769

 Copyright © Huawei Technologies Co., Ltd. 

16.7.1 Preconfiguring a Local Certificate 769
16.7.1.1 Configuring a PKI Entity 769
16.7.1.2 Configuring an RSA Key Pair 771
16.7.1.3 Configuring a PKI Entity to Obtain a CA Certificate 772
16.7.1.3.1 Downloading a CA Certificate for a PKI Entity 772
16.7.1.3.2 (Optional) Installing a CA Certificate for a PKI Entity 773
16.7.1.4 Verifying the Local Certificate Preconfiguration 774
16.7.2 Applying for and Updating Local Certificate 775
16.7.2.1 Applying for and Updating the Local Certificate Through SCEP 775
16.7.2.2 Applying for and Updating the Local Certificate Through CMPv2 779
16.7.2.3 Applying for the Local Certificate in Offline Mode 784
16.7.2.4 Verifying the Local Certificate Application and Update Configuration 786
16.7.3 (Optional) Downloading a Local Certificate 786
16.7.4 (Optional) Installing the Local Certificate 787
16.7.5 Verifying the CA and Local Certificates 789
16.7.5.1 Configuring Local Certificate Check 789
16.7.5.2 Checking the CA and Local Certificates 795
16.7.5.3 Verifying the CA and Local Certificate Configuration 796
16.7.6 Deleting the Local Certificate 796
16.7.7 Configuring the Extended Functions 797
16.7.7.1 Configuring Certificate Obtaining 797
16.7.7.2 Importing and Releasing a Peer Certificate 797
16.7.7.3 Configuring a Self-Signed Certificate or Local Certificate 798
16.7.7.4 Adding a PKI to a Specified VPN 799
16.8 Maintaining PKI 799
16.8.1 Checking PKI Information 799
16.8.2 Clearing PKI Information 800
16.9 Configuration Examples for PKI 800
16.9.1 Example for Configuring Automatic Local Certificate Application Using SCEP 800
16.9.2 Example for Configuring Initial Application of Local Certificate Using CMPv2 805
16.9.3 Example for Applying for the Local Certificate in Offline Mode 811
16.10 Troubleshooting PKI 815
16.10.1 A CA Certificate Failed to Be Obtained 815
16.10.2 A Local Certificate Failed to Be Obtained 816
16.11 FAQ About PKI 818
16.11.1 What Are the Differences Between CA, Local, and Self-Signed Certificates? 818
16.11.2 Which Certificate Formats Are Supported? 819
16.11.3 How Do I Manually Import Certificates and an RSA Key Pair? 820
**17 SSL Configuration 822**
17.1 Overview of SSL 822
17.2 Licensing Requirements and Limitations for SSL 824
17.3 Default Settings for SSL 825

 Copyright © Huawei Technologies Co., Ltd. 

17.4 Configuring a Server SSL Policy 825
17.5 Configuring a Client SSL Policy 827
17.6 Maintaining SSL 830
17.6.1 Viewing Statistics on SSL Connections 830
17.6.2 Deleting Statistics on SSL Connections 830
17.7 Configuration Examples for SSL 830
17.7.1 Example for Configuring a Server SSL Policy 830
17.7.2 Example for Configuring a Client SSL Policy 833
**18 HTTPS Configuration 838**
18.1 Overview of HTTPS 838
18.2 Licensing Requirements and Limitations for HTTPS 839
18.3 Configuring the Device as an HTTPS Server 839
18.4 Configuration Examples for HTTPS 840
18.4.1 Example for Configuring the Device as an HTTPS Server 840
**19 Keychain Configuration 843**
19.1 Overview of Keychains 843
19.2 Understanding Keychains 844
19.2.1 Basic Concepts of Keychains 844
19.2.2 Implementation of Keychains for a Non-TCP Application 846
19.2.3 Implementation of Keychains for TCP Applications 848
19.3 Application Scenarios for Keychains 850
19.4 Licensing Requirements and Limitations for Keychains 851
19.5 Configuring a Keychain 851
19.5.1 Creating a Keychain 852
19.5.2 Configuring a Key 853
19.5.3 Applying the Keychain 855
19.5.4 Verifying the Keychain Configuration 856
19.6 Configuration Examples for Keychains 856
19.6.1 Example for Applying the Keychain to RIP 856
19.6.2 Example for Applying the Keychain to BGP 859

 Copyright © Huawei Technologies Co., Ltd. 

# 1 AAA Configuration

## About This Chapter

1.1 Overview of AAA
1.2 Understanding AAA
1.3 Application Scenarios for AAA
1.4 Licensing Requirements and Limitations for AAA
1.5 Default Settings for AAA
1.6 Summary of AAA Configuration Tasks
1.7 Configuring AAA
1.8 Maintaining AAA
1.9 Configuration Examples for AAA
1.10 FAQ About AAA

## 1.1 Overview of AAA

### Definition

Authentication, Authorization, and Accounting (AAA) provide a user management mechanism, including the following functions:

- Authentication: verifies the identity of users for network access.
- Authorization: authorizes users to use particular services.
- Accounting: records the network resources used by users.

Users can use one or more security services provided by AAA. For example, if a company wants to authenticate employees that access certain network resources, the network administrator only needs to configure an authentication server. If the company also wants to record operations performed by employees on the network, an accounting server is needed.

 Copyright © Huawei Technologies Co., Ltd. 

In summary, AAA authorizes users to access specific resources and records user operations. AAA is widely used because it features good scalability and facilitates centralized user information management. AAA can be implemented using multiple protocols, and RADIUS is the most widely used protocol.

### Purpose

AAA prevents unauthorized users from logging in to a device and improves system security.

# 1.2 Understanding AAA

## 1.2.1 Domain-based User Management

An NAS performs domain-based user management. A domain is a group of users and each user belongs to a domain. A user uses only AAA configuration information in the domain to which the user belongs.

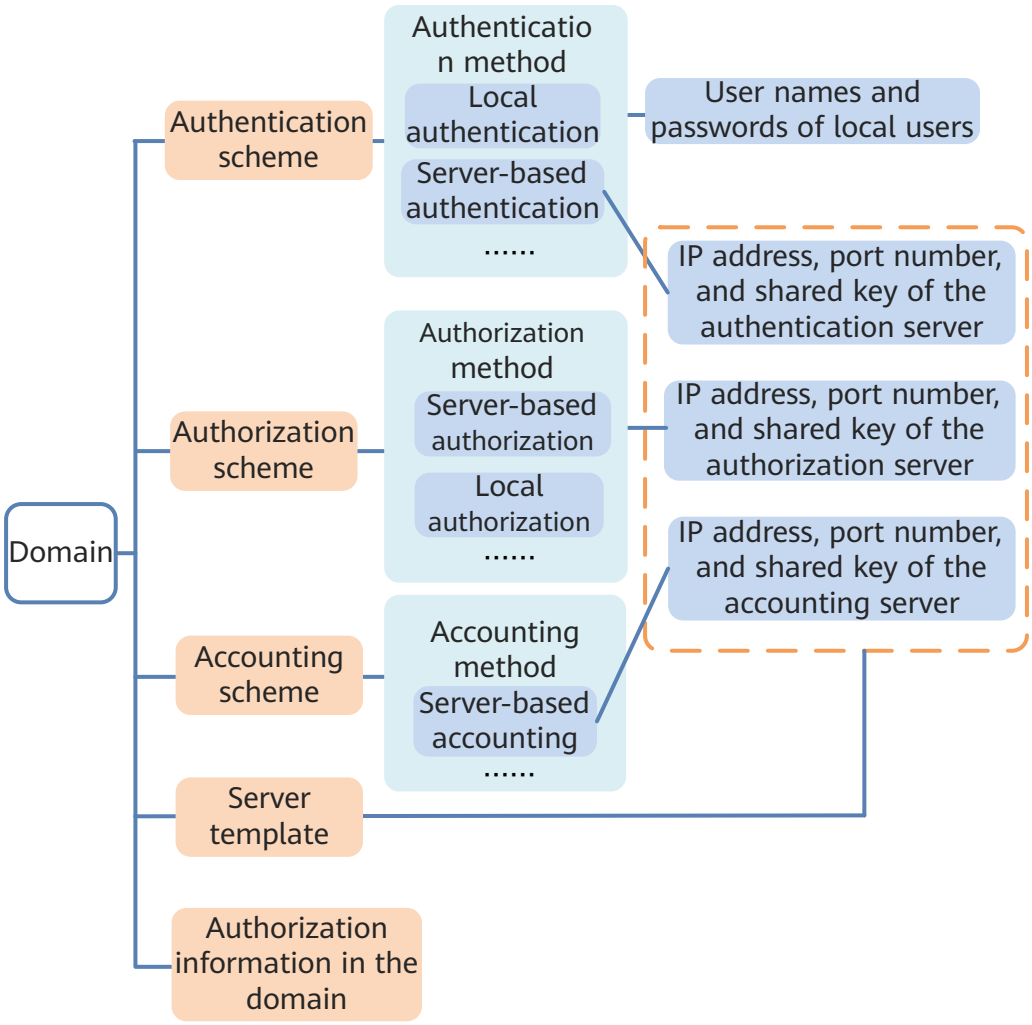
As shown in **Figure 1-1**, the domain manages configuration information including the AAA scheme, server template, and authorization information in a unified manner.

- AAA scheme: is divided into authentication, authorization, and accounting schemes that are used to define authentication, authorization, and accounting methods and the order in which the methods take effect. For details about the AAA scheme, see **1.2.2 AAA Scheme**.
- Server template: is used to configure a server for authentication, authorization, and accounting. When a server is configured for authorization, you can obtain the authorization information from the server and domain. For details, see **Figure 1-2**.

  If local authentication or authorization is used, you need to configure information related to the local user.
- Authorization information in the domain: can be configured in a domain.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 1-1** AAA configuration information in a domain

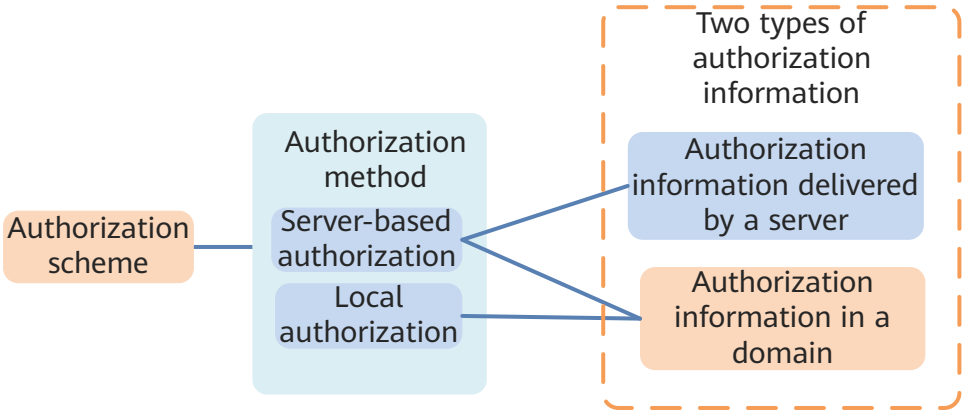



Authorization information can be delivered by a server or configured in a domain. Whether a user obtains authorization information delivered by a server or in a domain depends on the authorization method configured in the authorization scheme. For details, see **Figure 1-2**.

- If local authorization is used, the user obtains authorization information from the domain.
- If server-based authorization is used, the user obtains authorization information from the server or domain. Authorization information configured in a domain has lower priority than that delivered by a server. If the two types of authorization information conflicts, authorization information delivered by the server takes effect. If no conflict occurs, the two types of authorization information take effect simultaneously. In this manner, you can increase authorization flexibly by means of domain management, regardless of the authorization attributes provided by the AAA server.

 Copyright © Huawei Technologies Co., Ltd. 

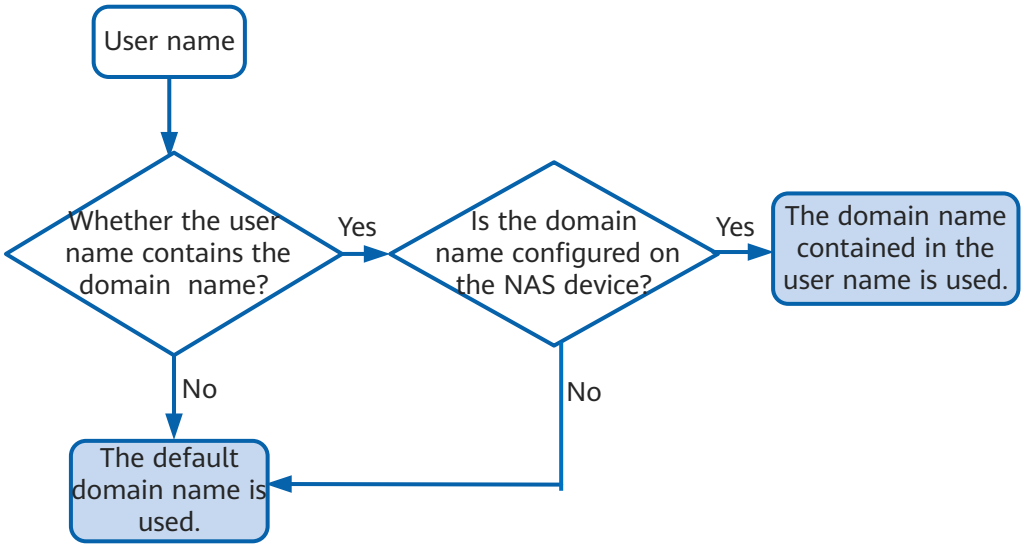
**Figure 1-2** Two types of authorization information




## Domain to Which a User Belongs

As shown in **Figure 1-3**, the domain to which a user belongs is determined by the user name for logging in to the NAS. If the user name does not contain the domain name or the domain name contained in the user name is not configured on the NAS, the NAS cannot determine the domain to which the user belongs. In this case, the NAS adds the user to the default domain based on the user type.

**Figure 1-3** Determining domains based on user names




As shown in **Table 1-1**, AAA divides users into administrators and access users to provide more refined and differentiated authentication, authorization, and accounting services. An NAS has two global default domains, namely, the global default administrative domain **default_admin** and the global default common domain **default**. The two domains are used as the global default domains for administrators and access users, respectively. Default configurations in the two domains are different.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

The accounting scheme **default** is bound to the two global default domains. Modifying the accounting scheme may affect configurations of the two domains.

The two global default domains cannot be deleted and can only be modified.

**Table 1-1** Global default domain

| User Type | User Access Mode | Global Default Domain | Default Configurations in the Global Default Domain | | |
|---|---|---|---|---|---|
| | | | Authentication Scheme | Accounting Scheme | Authorization Scheme |
| Administrator | Is also called a login user and refers to the user who can log in to NAS through FTP, HTTP, SSH, Telnet, and the console port. | default_admin | default (local authentication) | default (non-accounting) | N/A |
| Access user | Includes SSLVPN users and PPP users and NAC users (including 802.1X authenticated, MAC address authenticated, and Portal authenticated users). | default | radius (local authentication) | default (non-accounting) | N/A |

The global default domain can be customized based on actual requirements. The customized global default domain can be the global default common domain and the global default management domain at the same time.

You can run the **display aaa configuration** command to check the current global default common domain and the global default management domain on the NAS. The command output is as follows:

```
<Huawei> display aaa configuration
 Domain Name Delimiter            : @
 Domainname parse direction       : Left to right
 Domainname location              : After-delimiter
 Administrator user default domain: default_admin    //Global default management domain
 Normal user default domain       : default    //Global default common domain
```

For some access modes, you can specify the domain to which a user belongs using the command provided in the corresponding authentication profile to meet requirements of the user authentication management policy. For example, you can configure a default domain and a forcible domain for NAC access users on the NAS based on the authentication profile and specify the user type (802.1X, MAC address, or Portal authenticated user), achieving flexible configuration. The

 Copyright © Huawei Technologies Co., Ltd. 

forcible domain, default domain, and domain carried in the user name are listed in descending order of the priority.

Forcible domain with a specified authentication method in the authentication profile > Forcible domain in the authentication profile > Domain carried in the user name > Default domain with a specified authentication method in the authentication profile > Default domain in the authentication profile > Global default domain. Note that a forcible domain specified for MAC address authenticated users within a MAC address range has the highest priority and takes precedence over that configured in an authentication profile.

## Format of User Names Sent by an NAS to the RADIUS Server

NOTE

- Only RADIUS authentication supports modification of the user-entered original user names.
- You can change the user-entered original user name based on the RADIUS server template.

An NAS can determine whether a user name sent to the RADIUS server contains the domain name based on the RADIUS server requirements. By default, an NAS directly sends the user-entered original user name to the RADIUS server without changing it.

You can set the format of user names sent by an NAS to the RADIUS server using the commands in **Table 1-2**.

The following commands modify only the user name format in RADIUS packets sent to the RADIUS server and do not modify the user name format in EAP packets. During 802.1X authentication, the RADIUS server checks whether the user name carried in EAP packets is the same as that on the RADIUS server. Therefore, you cannot modify the original user name using the **radius-server user-name domain-included** or **undo radius-server user-name domain-included** command during 802.1X authentication; otherwise, authentication may fail.

**Table 1-2** Setting the format of user names sent by an NAS to the RADIUS server

| Command | User Name Format | User-entered User Name | User Name Sent by an NAS to the RADIUS Server |
| --- | --- | --- | --- |
| **radius-server user-name original** | User-entered original user name (default configuration) | user-name@huawei.com | user-name@huawei.com |
| | | user-name | user-name |
| **radius-server user-name domain-included** | Domain name included | user-name@huawei.com | user-name@huawei.com |
| | | user-name | user-name@default<br>Assume that users use the default domain **default**. |

 Copyright © Huawei Technologies Co., Ltd. 

| | | | |
|---|---|---|---|
| **undo radius-server user-name domain-included** | Domain name excluded | user-name@huawei.com | user-name |
| | | user-name | user-name |
| **undo radius-server user-name domain-included except-eap** | Domain name excluded<br>**NOTE**<br>This command takes effect only for non-EAP authenticated users. | user-name@huawei.com | user-name |
| | | user-name | user-name |

# 1.2.2 AAA Scheme

During AAA implementation, you can define a set of AAA configuration policies using an AAA scheme. An AAA scheme contains a collection of authentication, authorization, and accounting methods defined on an NAS. Such methods can be used in combination depending on access features of users and security requirements.

## 1.2.2.1 Authentication Scheme

An authentication scheme is used to define methods for user authentication and the order in which authentication methods take effect. An authentication scheme is applied to a domain. It is combined with the authorization scheme, accounting scheme, and server template in the domain for user authentication, authorization, and accounting.

### Authentication Methods Supported by a Device

- RADIUS authentication: User information is configured on the RADIUS server through which user authentication is performed.
- HWTACACS authentication: User information is configured on the HWTACACS server through which user authentication is performed.
- Local authentication: The device functions as an authentication server and user information is configured on the device. This mode features fast processing and low operation costs. However, the information storage capacity is subject to the device hardware.
- Non-authentication: Users are completely trusted without validity check. This mode is rarely used.

### Order in Which Authentication Methods Take Effect

An authentication scheme enables you to designate one or more authentication methods to be used for authentication, thus ensuring a backup system for authentication in case the initial method does not respond. An NAS uses the first

 Copyright © Huawei Technologies Co., Ltd. 

method listed in the scheme to authenticate users; if that method does not respond, the NAS selects the next authentication method in the authentication scheme. This process continues until there is successful communication with a listed authentication method or the authentication method list is exhausted, in which case authentication fails.

NOTE

The NAS attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle — meaning that the AAA server responds by denying the user access — the authentication process stops and no other authentication methods are attempted.

### 1.2.2.2 Authorization Scheme

An authorization scheme is used to define methods for user authorization and the order in which authorization methods take effect. An authorization scheme is applied to a domain. It is combined with the authentication scheme, accounting scheme, and server template in the domain for user authentication, authorization, and accounting.

## Authorization Methods Supported by a Device

- HWTACACS authorization: An HWTACACS server is used to authorize users.
- Local authorization: The device functions as an authorization server to authorize users based on user information configured on the device.
- Non-authorization: Authenticated users have unrestricted access rights on a network.
- if-authenticated authorization: If passing authentication, a user passes authorization; otherwise, the user fails authorization. This mode applies to scenarios where users must be authenticated and the authentication process can be separated from the authorization process.

NOTE

RADIUS authentication is combined with authorization and cannot be separated. If authentication succeeds, authorization also succeeds. When RADIUS authentication is used, you do not need to configure an authorization scheme.

In addition, the "authentication + rights level" method is typically used to control access of the administrators (login users) to the device, improving the device operation security. Authentication restricts the administrators' access to the device and the rights level defines commands that the administrators can enter after logging in to the device. For details about the method, see CLI Login Configuration in *Huawei AR Series V200R010 CLI-based configuration - Basic Configuration Guide*.

## Order in Which Authorization Methods Take Effect

An authorization scheme enables you to designate one or more authorization methods to be used for authorization, thus ensuring a backup system for authorization in case the initial method does not respond. The first method listed in the scheme is used to authorize users; if that method does not respond, the next authorization method in the authentication scheme is selected. If the initial

 Copyright © Huawei Technologies Co., Ltd. 

method responds with an authorization failure message, the AAA server refuses to provide services for the user. In this case, authorization ends and the next listed method is not used.

## Authorization Information

Authorization information can be delivered by a server or configured in a domain. Whether a user obtains authorization information delivered by a server or in a domain depends on the authorization method configured in the authorization scheme. For details, see **Figure 1-4**.

- If local authorization is used, the user obtains authorization information from the domain.
- If server-based authorization is used, the user obtains authorization information from the server or domain. Authorization information configured in a domain has lower priority than that delivered by a server. If the two types of authorization information conflicts, authorization information delivered by the server takes effect. If no conflict occurs, the two types of authorization information take effect simultaneously. In this manner, you can increase authorization flexibly by means of domain management, regardless of the authorization attributes provided by the AAA server.

**Figure 1-4** Two types of authorization information

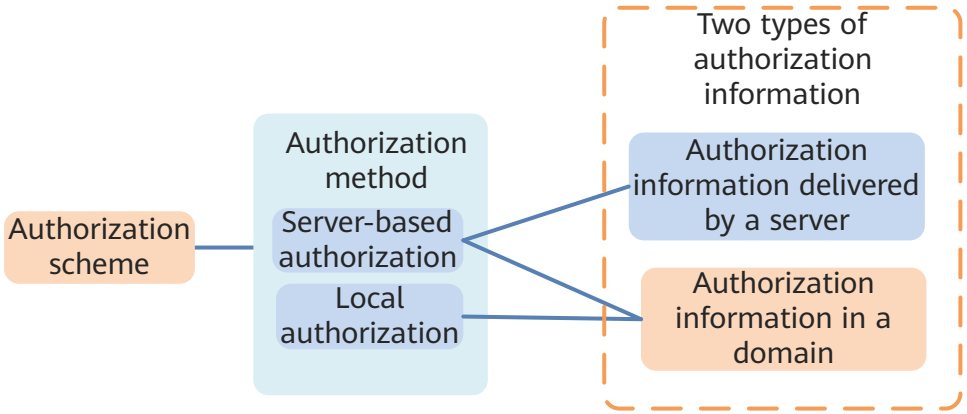



**Table 1-3** shows authorization information typically used by a server. **Table 1-4** shows authorization information that can be configured in a domain.

**Table 1-3** Common authorization information of a RADIUS server

| Authorization Information | Description |
| --- | --- |
| ACL number | Is delivered by the server. You need to configure ACL number-related rules on the NAS. |
| ACL rule | Is directly delivered by the server. As defined in the rule, users can access all network resources included in the ACL. You do not need to configure the corresponding ACL on the NAS. |


Copyright © Huawei Technologies Co., Ltd.

| Authorization Information | Description |
| --- | --- |
| VLAN | If dynamic VLAN delivery is configured on the server, authorization information sent to the NAS includes the VLAN attribute. After the NAS receives the authorization information, it changes the VLAN to which the user belongs to the delivered VLAN.<br>The delivered VLAN does not change or affect the interface configuration. The delivered VLAN, however, takes precedence over the user-configured VLAN. That is, the delivered VLAN takes effect after the authentication succeeds, and the user-configured VLAN takes effect after the user goes offline. |
| User group | The server delivers the user group name to the NAS. You need to configure the corresponding group and network resources in the group on the NAS. |
| CAR | The server delivers authorization to control the committed information rate (CIR), peak information rate (PIR), committed burst size (CBS), and peak burst size (PBS) for access between the user and NAS. |
| Administrator level | Priority of an administrator (such as a Telnet user) delivered by the server. The priority ranges from 0 to 15. The value greater than or equal to 16 is invalid. |
| Service scheme | Name of a service scheme delivered by the server. You need to configure the corresponding service scheme and the network authorization and policy in the scheme on the NAS. |
| Idle-cut | Idle-cut time delivered by the server. After a user goes online, if the consecutive non-operation period or the duration when traffic is lower than a specified value exceeds the idle-cut time, the user is disconnected. |
| Reauthentication or forcible logout | Remaining service availability period delivered by the server. If the period expires, reauthentication is performed for the user or the user is forced to go offline according to the server-delivered action. |

 Copyright © Huawei Technologies Co., Ltd. 

**Table 1-4** Authorization information that can be configured in a domain

| Authorization Parameter | Description |
| --- | --- |
| VLAN | VLAN-based authorization is easy to deploy and requires low maintenance costs. It applies to scenarios where employees in an office or a department have the same access rights.<br>In local authorization, you only need to configure VLANs and corresponding network resources in the VLAN on the NAS.<br>If a user uses Portal authentication or a hybrid authentication mode (including Portal authentication), the NAS cannot perform VLAN-based authorization for the user.<br>After a user obtains VLAN-based authorization, the user needs to manually request an IP address using DHCP. |
| Service scheme | A service scheme and corresponding network resources in the scheme need to be configured on the NAS. |
| User group | A user group consists of users (terminals) with the same attributes such as the role and rights. For example, you can divide users on a campus network into the R&D group, finance group, marketing group, and guest group based on the enterprise department structure, and grant different security policies to different departments.<br>You need to configure a user group and corresponding network resources in the group on the NAS. |

### 1.2.2.3 Accounting Scheme

An accounting scheme is used to define a user accounting method. An accounting scheme is applied to a domain. It is combined with the authentication scheme, authorization scheme, and server template in the domain for user authentication, authorization, and accounting.

#### Accounting Methods Supported by a Device

- RADIUS accounting: A RADIUS server is used to perform user accounting.
- HWTACACS accounting: An HWTACACS server is used to perform user accounting.
- Non-accounting: Users can access a network without being charged.

#### Order in Which Accounting Methods Take Effect

You can only specify an accounting method at one time in an accounting scheme.

RADIUS accounting packets in **1.2.4.2 RADIUS Packets** indicate that accounting packets are divided into Accounting-Request and Accounting-Response packets.

 Copyright © Huawei Technologies Co., Ltd. 

Accounting succeeds if each Accounting-Request packet sent by a device is responded by the server with an Accounting-Response packet. If no Accounting-Response packet is received from the server, accounting fails.

After the accounting function is enabled, the device sends Accounting-Request packets recording user activities to the AAA server. The AAA server then performs user accounting and auditing based on information in the packets. Take RADIUS accounting as an example. Accounting-Request packets are divided into three types:

- Accounting-Request (Start) packet: When a user is successfully authenticated and begins to access network resources, the device sends an Accounting-Request (Start) packet to the RADIUS server.
- Accounting-Request (Stop) packet: When a user is disconnected proactively (or forcibly by the NAS), the device sends an Accounting-Request (Stop) packet to the server.
- Accounting-Request (Interim-update) packet: To reduce accounting deviation and ensure that the accounting server can receive Accounting-Request (Stop) packets and stop user accounting, you can configure the real-time accounting function on the device. In this case, the device periodically sends an Accounting-Request (Interim-update) packet to the RADIUS server.

Typically, each Accounting-Request packet sent by a device is responded by the server with an Accounting-Response packet. If the device does not receive a corresponding Accounting-Response packet due to network faults, accounting fails. In this case, the device determines whether the user can still be online depending on the type of the Accounting-Request packet as follows:

- Accounting-start failure: The user goes offline by default.
- Real-time accounting failure: The user is allowed to be online by default.
- stop_acct_fail: The device retransmits the Accounting-Request(Stop) packet.

# 1.2.3 Local Authentication and Authorization

## Local AAA Server

A device functioning as an AAA server is called a local AAA server that performs user authentication and authorization and cannot perform user accounting.

Similar to the remote AAA server, the local AAA server requires the local user names, passwords, and authorization information of local users. The authentication and authorization speed of a local AAA server is faster than that of a remote AAA server, which reduces operation costs. However, the information storage capacity of a local AAA server is subject to the device hardware.

## Security Policy for Local User Password

### Password Length and Complexity

When an administrator creates local users on a device, the length and complexity of local users' passwords have been controlled by commands on the device. The complexity check requires that the password must be a combination of at least two of the following: digits, lowercase letters, uppercase letters, and special characters. In addition, a password must consist of at least eight characters.

 Copyright © Huawei Technologies Co., Ltd. 

**Password Validity Period**

After the local administrator password policy is enabled, the local administrator can set the password validity period. The default validity period is 90 days and can be changed.

If the password of a local user expires and the local user still uses this password to log in to the device, the device prompts the user that the password has expired, and asks the user whether to change the password. The device then performs the following operations depending on the user selection:

- If the user enters **Y**, the user needs to enter the old password, new password, and confirm password. The password can be successfully changed only when the old password is correct and the new password and confirm password are the same and meet password length and complexity requirements.
- If the user enters **N** or fails to change the password, the user cannot log in to the device.

The device also supports the password expiration prompt function. When a user logs in to the device, the device checks how many days the password is valid for. If the number of days is less than the prompt days set in the command, the device notifies the user how long the password will expire and asks the user whether to change the password.

- If the user changes the password, the device records the new password and modification time.
- If the user does not change the password or fails to change the password, the user can still log in to the device as long as the password has not expired.

**Password Modification Policy**

During password modification, you are not advised to use old passwords. By default, the new password cannot be the same as those used for the last five times.

The local administrator can change the password of an equal- or lower-level local user.

# 1.2.4 RADIUS AAA

## 1.2.4.1 Overview of RADIUS

AAA can be implemented using multiple protocols. RADIUS is most frequently used in actual scenarios.

RADIUS is a protocol that uses the client/server model in distributed mode and protects a network from unauthorized access. It is often used on networks that require high security and control remote user access. It defines the UDP-based RADIUS packet format and transmission mechanism, and specifies UDP ports 1812 and 1813 as the default authentication and accounting ports respectively.

At the very beginning, RADIUS was only the AAA protocol used for dial-up users. As the user access mode diversifies, such as Ethernet access, RADIUS can also be applied to these access modes. RADIUS provides the access service through

 Copyright © Huawei Technologies Co., Ltd. 

authentication and authorization and records the network resource usage of users through accounting.

RADIUS has the following characteristics:

- Client/Server model
- Secure message exchange mechanism
- Fine scalability

## Client/Server Model

- RADIUS client

  RADIUS clients run on the NAS to transmit user information to a specified RADIUS server and process requests (for example, permit or reject user access requests) based on the responses from the server. RADIUS clients can locate at any node on a network.

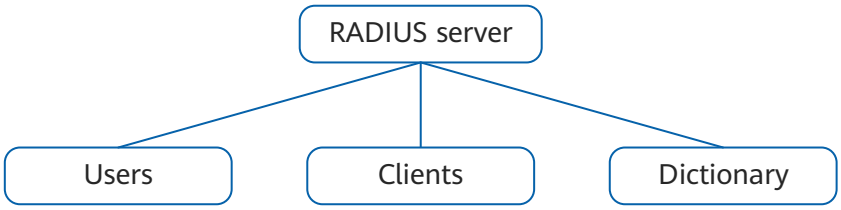
  As a RADIUS client, a device supports:

  – standard RADIUS protocol and its extensions, including RFC 2865 and RFC 2866
  – Huawei extended RADIUS attributes
  – RADIUS server status detection
  – retransmission of Accounting-Request(Stop) packets in the local buffer
  – active/standby and load balancing functions between RADIUS servers

- RADIUS server

  RADIUS servers typically run on central computers and workstations to maintain user authentication and network service access information. The servers receive connection requests from users, authenticate the users, and send all required information (such as permitting or rejecting authentication requests) to the clients. A RADIUS server generally needs to maintain three databases, as shown in **Figure 1-5**.

  **Figure 1-5** Databases maintained by a RADIUS server

  – Users: This database stores user information such as user names, passwords, protocols, and IP addresses.
  – Clients: This database stores RADIUS client information, such as the shared keys and IP addresses.
  – Dictionary: This database stores the attributes in the RADIUS protocol and their value descriptions.

 Copyright © Huawei Technologies Co., Ltd. 

## Secure Message Exchange Mechanism

Authentication messages between a RADIUS server and RADIUS clients are exchanged using a shared key. The shared key is a character string that is transmitted in out-of-band mode, is known to both clients and the server, and does not need to be transmitted independently on the network.

A RADIUS packet has a 16-octet Authenticator field that contains the digital signature data of the whole packet. The signature data is calculated using the MD5 algorithm and shared key. The RADIUS packet receiver needs to verify whether the signature is correct and discards the packet if the signature is incorrect.

This mechanism improves security of message exchange between RADIUS clients and the RADIUS server. In addition, user passwords contained in RADIUS packets are encrypted using shared keys before the packets are transmitted to prevent the user passwords from being stolen during transmission on an insecure network.

## Fine Scalability

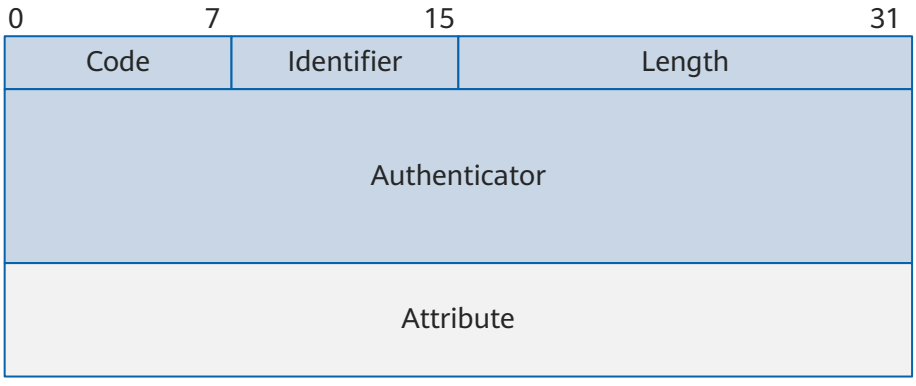
A RADIUS packet consists of a packet header and a certain number of attributes. The protocol implementation remains unchanged even if new attributes are added to a RADIUS packet.

## 1.2.4.2 RADIUS Packets

## RADIUS Packet Format

RADIUS is based on the UDP protocol. **Figure 1-6** shows the RADIUS packet format.

**Figure 1-6** RADIUS packet format




Each RADIUS packet contains the following information:

- Code: The Code field is one octet and identifies type of a RADIUS packet. Value of the Code field varies depending on the RADIUS packet type. For example, the value 1 indicates an Access-Request packet and the value 2 indicates an Access-Accept packet.

 Copyright © Huawei Technologies Co., Ltd. 

- Identifier: The identifier field is one octet, and helps the RADIUS server match requests and responses and detect duplicate requests retransmitted within a certain period. After a client sends a request packet, the server sends a reply packet with the same Identifier value as the request packet.
- Length: The Length field is two octets and specifies length of a RADIUS packet. Octets outside the range of the Length field must be treated as padding and ignored on reception. If a packet is shorter than the Length field, it must be silently discarded.
- Authenticator: The Authenticator field is 16 octets. This value is used to authenticate the reply from the RADIUS server and is used in the password hiding algorithm.
- Attribute: This field is variable in length. RADIUS attributes carry the specific authentication, authorization, accounting information and configuration details for the request and reply packets. The Attribute field may contain multiple attributes, each of which consists of Type, Length, and Value. For details, see **1.2.4.8 RADIUS Attributes**.
  - Type: The Type field is one octet and indicates the RADIUS attribute ID. The value ranges from 1 to 255.
  - Length: The Length field is one octet, and indicates the length of the RADIUS attribute (including the Type, Length and Value fields). The Length is measured in octets.
  - Value: The maximum length of the Value field is 253 bytes. The Value field contains information specific to the RADIUS attribute. The format and length of the Value field is determined by the Type and Length fields.

## RADIUS Packet Type

RADIUS defines 16 types of packets. **Table 1-5** describes types of the authentication packets, **Table 1-6** describes types of the accounting packets. For RADIUS CoA/DM packets, see **1.2.4.7 RADIUS CoA/DM**.

**Table 1-5** RADIUS authentication packet

| Packet Name | Description |
| --- | --- |
| Access-Request | Access-Request packets are sent from a client to a RADIUS server and is the first packet transmitted in a RADIUS packet exchange process. This packet conveys information (such as the user name and password) used to determine whether a user is allowed access to a specific NAS and any special services requested for that user. |
| Access-Accept | After a RADIUS server receives an Access-Request packet, it must send an Access-Accept packet if all attribute values in the Access-Request packet are acceptable (authentication success). The user is allowed access to requested services only after the RADIUS client receives this packet. |
| Access-Reject | After a RADIUS server receives an Access-Request packet, it must send an Access-Reject packet if any of the attribute values are not acceptable (authentication failure). |

 Copyright © Huawei Technologies Co., Ltd. 

| Packet Name | Description |
| --- | --- |
| Access-Challenge | During an EAP relay authentication, when a RADIUS server receives an Access-Request packet carrying the user name from a client, it generates a random MD5 challenge and sends the MD5 challenge to the client through an Access-Challenge packet. The client encrypts the user password using the MD5 challenge, and then sends the encrypted password in an Access-Request packet to the RADIUS server. The RADIUS server compares the encrypted password received from the client with the locally encrypted password. If they are the same, the server determines the user is valid. |

**Table 1-6** RADIUS accounting packet

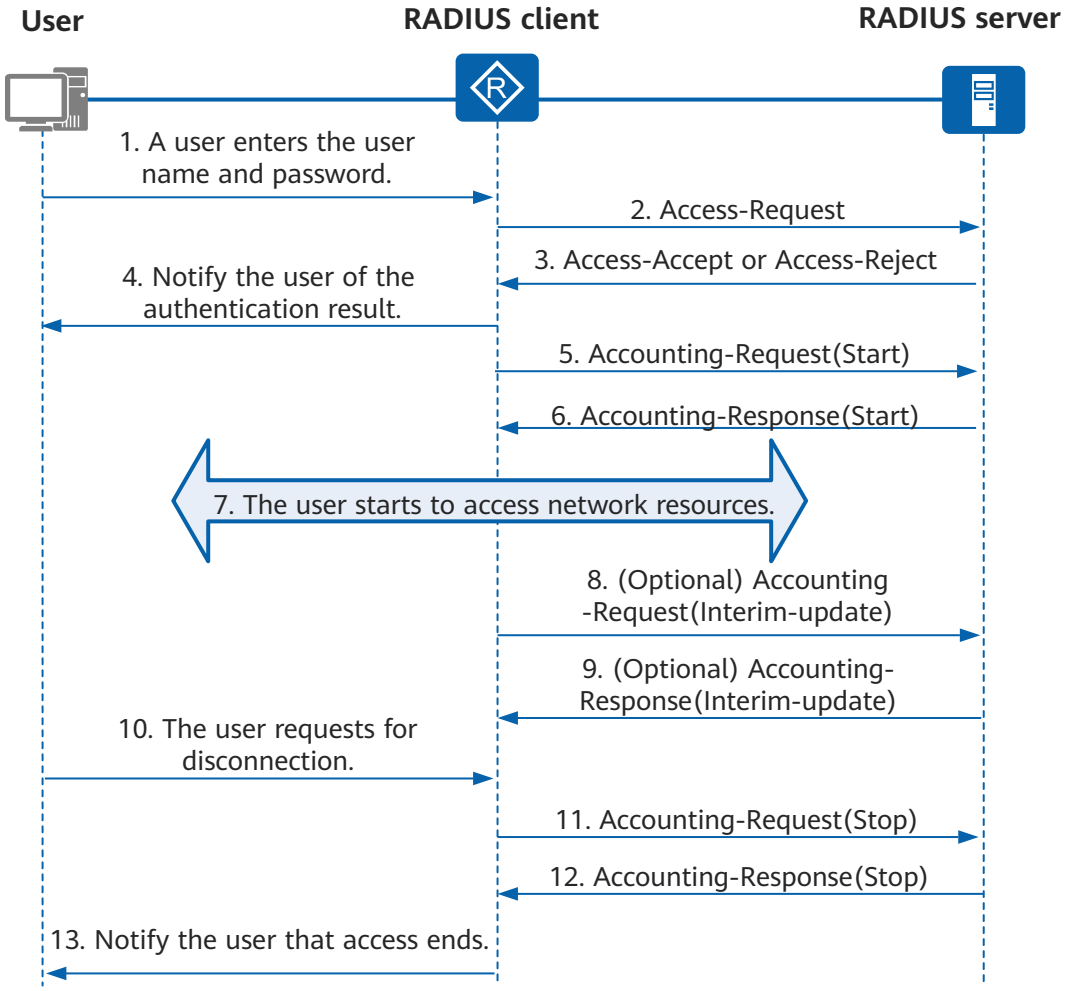
| Packet Name | Description |
| --- | --- |
| Accounting-Request(Start) | If a RADIUS client uses RADIUS accounting, the client sends this packet to a RADIUS server before accessing network resources. |
| Accounting-Response(Start) | The RADIUS server must send an Accounting-Response(Start) packet after the server successfully receives and records an Accounting-Request(Start) packet. |
| Accounting-Request(Interim-update) | You can configure the real-time accounting function on a RADIUS client to prevent the RADIUS server from continuing user accounting if it fails to receive the Accounting-Request(Stop) packet. The client then periodically sends Accounting-Request(Interim-update) packets to the server, reducing accounting deviation. |
| Accounting-Response(Interim-update) | The RADIUS server must send an Accounting-Response(Interim-update) packet after the server successfully receives and records an Accounting-Request(Interim-update) packet. |
| Accounting-Request(Stop) | When a user goes offline proactively or is forcibly disconnected by the NAS, the RADIUS client sends this packet carrying the network resource usage information (including the online duration and number of incoming/outgoing bytes) to the RADIUS server, requesting the server to stop accounting. |
| Accounting-Response(Stop) | The RADIUS server must send an Accounting-Response(Stop) packet after receiving an Accounting-Request(Stop) packet. |

 Copyright © Huawei Technologies Co., Ltd. 

### 1.2.4.3 RADIUS Authentication, Authorization, and Accounting Process

A device that functions as a RADIUS client collects user information, including the user name and password, and sends the information to the RADIUS server. The RADIUS server then authenticates users according to the information, after which it performs authorization and accounting for the users. **Figure 1-7** shows the information exchange process between a user, a RADIUS client, and a RADIUS server.

**Figure 1-7** RADIUS authentication, authorization, and accounting process




1. A user needs to access a network and sends a connection request containing the user name and password to the RADIUS client (device).
2. The RADIUS client sends a RADIUS Access-Request packet containing the user name and password to the RADIUS server.
3. The RADIUS server verifies the user identity:
   - If the user identity is valid, the RADIUS server returns an Access-Accept packet to the RADIUS client to permit further operations of the user. The Access-Accept packet contains authorization information because RADIUS provides both authentication and authorization functions.


Copyright © Huawei Technologies Co., Ltd.

- If the user identity is invalid, the RADIUS server returns an Access-Reject packet to the RADIUS client to reject access from the user.

4. The RADIUS client notifies the user of whether authentication is successful.
5. The RADIUS client permits or rejects the user access request according to the authentication result. If the access request is permitted, the RADIUS client sends an Accounting-Request (Start) packet to the RADIUS server.
6. The RADIUS server sends an Accounting-Response (Start) packet to the RADIUS client and starts accounting.
7. The user starts to access network resources.
8. (Optional) If interim accounting is enabled, the RADIUS client periodically sends an Accounting-Request (Interim-update) packet to the RADIUS server, preventing incorrect accounting result caused by unexpected user disconnection.
9. (Optional) The RADIUS server returns an Accounting-Response (Interim-update) packet and performs interim accounting.
10. The user sends a logout request.
11. The RADIUS client sends an Accounting-Request (Stop) packet to the RADIUS server.
12. The RADIUS server sends an Accounting-Response (Stop) packet to the RADIUS client and stops accounting.
13. The RADIUS client notifies the user of the processing result, and the user stops accessing network resources.

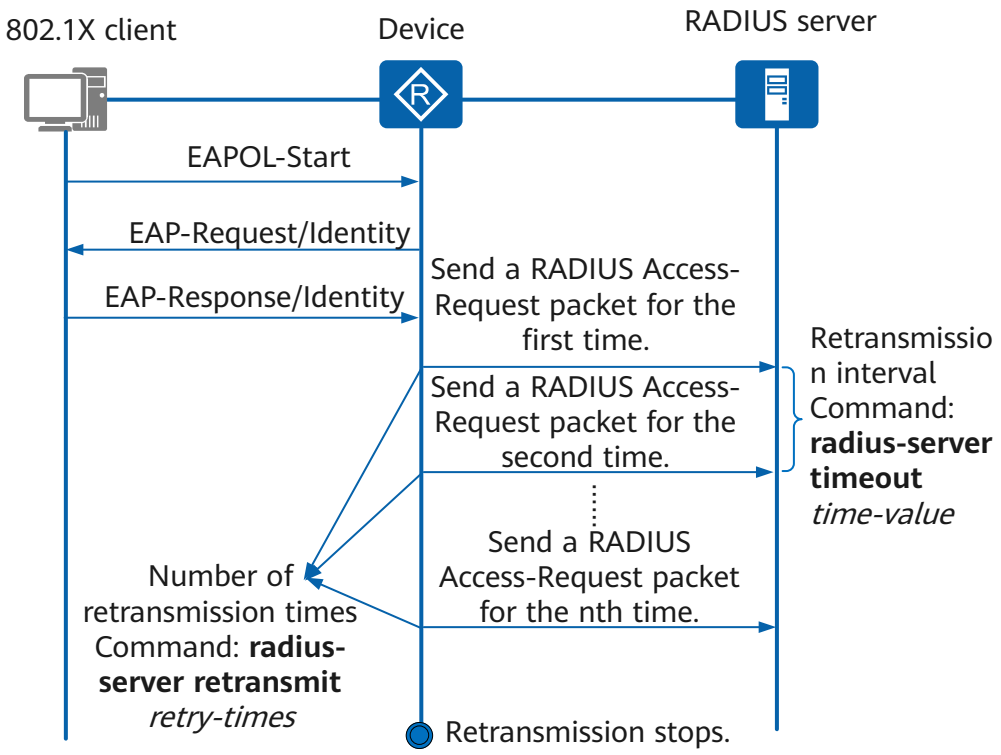
### 1.2.4.4 RADIUS Packet Retransmission Mechanism

When a user is authenticated, a device sends an Access-Request packet to the RADIUS server. To ensure that the device can receive a response packet from the server even if a network fault or delay occurs, a retransmission upon timeout mechanism is used. The retransmission times and retransmission interval are controlled using timers.

As shown in **Figure 1-8**, 802.1X authentication and client-initiated authentication are used as an example. After receiving an EAP packet (EAP-Response/Identity) containing the user name of the client, the device encapsulates the packet into a RADIUS Access-Request packet and sends the packet to the RADIUS server. The retransmission timer is enabled at the same time. The retransmission timer is composed of the retransmission interval and retransmission times. If the device does not receive any response packet from the RADIUS server when the retransmission interval expires, it sends a RADIUS Access-Request packet again.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 1-8** RADIUS authentication packet retransmission flowchart




The device stops packet retransmission if any of the following conditions is met:

- The device receives a response packet from the RADIUS server. It then stops packet retransmission and marks the RADIUS server status as Up.
- The device detects that the RADIUS server status is Down. After the device marks the RADIUS server status as Down:
  - If the number of retransmitted packets has reached the upper limit, the device stops packet retransmission and retains the RADIUS server status to Down.
  - If the number of retransmitted packets has not reached the upper limit, the device retransmits an Access-Request packet once again to the RADIUS server. If the device receives a response packet from the server, it stops packet retransmission and restores the RADIUS server status to Up. Otherwise, it still stops packet retransmission and retains the RADIUS server status to Down.
- The number of retransmitted packets has reached the upper limit. The device then stops packet retransmission and performs the following:
  - If the device receives a response packet from the RADIUS server, it marks the RADIUS server status as Up.
  - If the device has detected that the RADIUS server status is Down, it marks the server status as Down.
  - If the device receives no response packet from the RADIUS server and does not detect that the server status is Down, the device does not change the server status. Actually, the server does not respond.


Copyright © Huawei Technologies Co., Ltd.

NOTE

The device does not definitely mark the status of the server that does not respond as Down. The device marks the server status as Down only if the corresponding conditions are met.

For the RADIUS server status introduction and conditions for a device to mark the server status as Down, see **1.2.4.6 RADIUS Server Status Detection**.

RADIUS packet retransmission discussed here applies only to a single server. If multiple servers are configured in a RADIUS server template, the overall retransmission period depends on the retransmission interval, retransmission times, RADIUS server status, number of servers, and algorithm for selecting the servers.

You can set the timer using the following commands:

| Command | Description |
| --- | --- |
| **radius-server retransmit** *retry-times* | Specifies the retransmission times. The default value is 3. |
| **radius-server timeout** *time-value* | Specifies the retransmission interval. The default value is 5 seconds. |

## 1.2.4.5 RADIUS Server Selection Mechanism

Typically, multiple RADIUS servers are deployed on a large-scale enterprise network. If a server is faulty, user access will not be disrupted. In addition, load balancing is performed between these servers, preventing resources of a single server from being exhausted in the event that a large number of users access the network. If multiple servers are configured in a RADIUS server template and a device needs to send a packet to a server, select one of the following algorithms to select the RADIUS server based on the command configuration.

- RADIUS server primary/secondary algorithm (default)
- RADIUS server load balancing algorithm

In addition, the algorithm for selecting a RADIUS server can be set to the single user-based or packet-based algorithm. If the algorithm for selecting a RADIUS server is set to the single user-based algorithm, authentication server information is saved in the authentication phase, and the device preferentially sends an accounting request to the accounting server in the accounting phase when the authentication server is also the accounting server. If the algorithm for selecting a RADIUS server is set to the packet-based algorithm, authentication server information is not saved in the authentication phase, and the accounting server is reselected in the accounting phase, which may result in that authentication and accounting for a user is not performed on the same server.

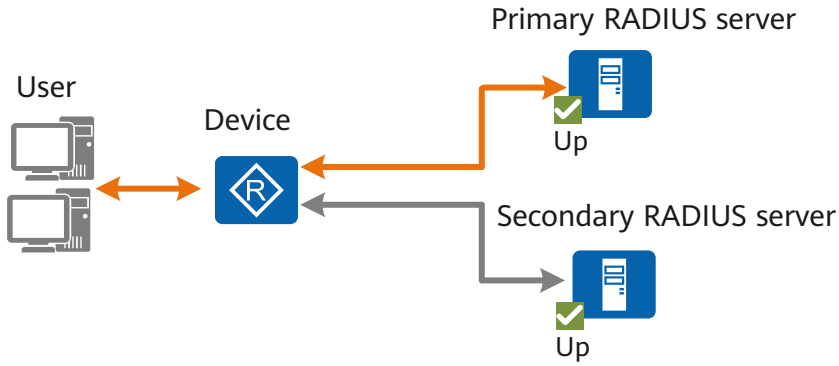
### RADIUS Server Primary/Secondary Algorithm

The primary and secondary roles are determined by the weights configured for the RADIUS authentication servers or RADIUS accounting servers. The server with the

 Copyright © Huawei Technologies Co., Ltd. 

largest weight is the primary server. If the weight values are the same, the earliest configured server is the primary server. As shown in **Figure 1-9**, the device preferentially sends an authentication or accounting packet to the primary server among all servers in Up status. If the primary server does not respond, the device then sends the packet to the secondary server.

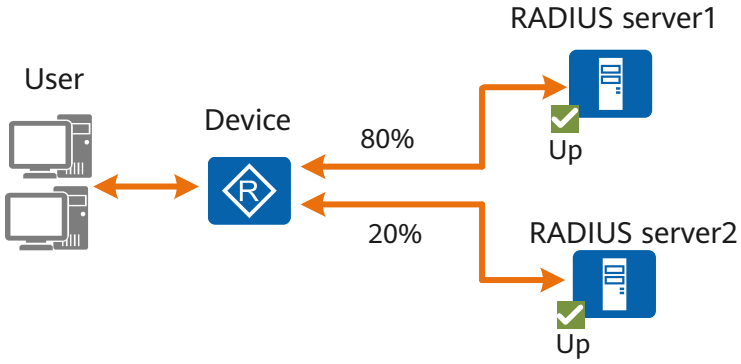
**Figure 1-9** Diagram for the RADIUS server primary/secondary algorithm




## RADIUS Server Load Balancing Algorithm

If this algorithm is used and a device sends an authentication or accounting packet to a server, the device selects a server based on the weights configured for the RADIUS authentication servers or RADIUS accounting servers. As shown in **Figure 1-10**, RADIUS server1 is in Up status and its weight is 80, and RADIUS server2 is also in Up status and its weight is 20. The possibility for the device to send the packet to RADIUS server1 is 80% [80/(80 + 20)], and that for RADIUS server2 is 20% [20/(80 + 20)].

**Figure 1-10** Diagram for the RADIUS server load balancing algorithm




Regardless of which algorithm is used, if all the servers in Up status do not respond to a packet sent by a device, the device retransmits the packet to a server among the servers whose status is originally marked as Down (to which the device has not sent any authentication or accounting packets) based on the server weight. If the device does not receive any response in the current authentication mode, the backup authentication mode is used, for example, local authentication mode. The backup authentication mode needs to be already configured in the authentication scheme. Otherwise, the authentication process ends.

 Copyright © Huawei Technologies Co., Ltd. 

## 1.2.4.6 RADIUS Server Status Detection

Availability and maintainability of a RADIUS server are the prerequisites of user access authentication. If a device cannot communicate with the RADIUS server, the server cannot perform authentication or authorization for users. To resolve this issue, the device supports the user escape function upon transition of the RADIUS server status to Down. To be specific, if the RADIUS server goes Down, users cannot be authorized by the server but still have certain network access rights.

The user escape function upon transition of the RADIUS server status to Down can be enabled only after the device marks the RADIUS server status as Down. If the RADIUS server status is not marked as Down and the device cannot communicate with the RADIUS server, users cannot be authorized by the server and the escape function is also unavailable. As a result, users have no network access rights. Therefore, the device must be capable of detecting the RADIUS server status in a timely manner. If the device detects that the RADIUS server status transitions to Down, users can obtain escape rights; if the device detects that the RADIUS server status reverts to Up, escape rights are removed from the users and the users are reauthenticated.

This section contains the following contents:

- **RADIUS Server Status**
- **Conditions for Marking the RADIUS Server Status as Down**
- **Automatic Detection**
- **Consecutive Processing After the RADIUS Server Status Is Marked as Down**

### RADIUS Server Status

A device can mark the RADIUS server status as Up, Down, or Force-up. The following table lists descriptions of the three RADIUS server status and their corresponding scenarios.

| Status | Whether the RADIUS Server Is Available | Condition for Switching the Server Status |
| --- | --- | --- |
| Up | The RADIUS server is available. | • The device initially marks the RADIUS server status as Up.<br>• The device marks the RADIUS server status as Up if receiving packets from the server. |
| Down | The RADIUS server is unavailable. | The conditions for marking the RADIUS server status as Down are met. |

 Copyright © Huawei Technologies Co., Ltd. 

| Status | Whether the RADIUS Server Is Available | Condition for Switching the Server Status |
| --- | --- | --- |
| Force-up | When no RADIUS server is available, the device selects the RADIUS server in Force-up status. | The device marks the RADIUS server status as Force-up if the timer specified by **dead-time** expires. |

The RADIUS server status is initially marked as Up. After a RADIUS Access-Request packet is received and the conditions for marking the RADIUS server status as Down are met, the RADIUS server status transitions to Down. The RADIUS Access-Request packet that triggers the server status transition can be sent during user authentication or constructed by the administrator. For example, the RADIUS Access-Request packet can be a test packet sent when the **test-aaa** command is run or detection packet sent during automatic detection.

The device changes toe RADIUS server status from Down to Up or to Force-up in the following scenarios:

- Down to Force-up: The timer specified by **dead-time** starts after the device marks the RADIUS server status as Down. The timer indicates the duration for which the server status remains Down. After the timer expires, the device marks the RADIUS server status as Force-up. If a new user needs to be authenticated in RADIUS mode and no RADIUS server is available, the device attempts to re-establish a connection with a RADIUS server in Force-up status.
- Down to Up: After receiving packets from the RADIUS server, the device changes the RADIUS server status from Down to Up. For example, after automatic detection is configured, the device receives response packets from the RADIUS server.

## Conditions for Marking the RADIUS Server Status as Down

Whether the status of a RADIUS server can be marked as Down depends on the following factors:

- Number of times the RADIUS Access-Request packet is sent
- Interval of sending the RADIUS Access-Request packet
- Interval of detecting the RADIUS server status
- Maximum number of consecutive unacknowledged packets in each detection interval

As shown in **Figure 1-11**, the conditions for marking the RADIUS server status as Down are as follows:

1. In a detection interval, if the number of times the device receives no response packet after sending RADIUS Access-Request packets (n) is greater than or equal to the maximum number of consecutive unacknowledged packets (*dead-count*), the device records a communication interruption.
2. If the device records communication interruptions with one RADIUS server in consecutive two detection intervals, the device considers that the RADIUS

 Copyright © Huawei Technologies Co., Ltd. 

server is unavailable and the conditions for the device to mark the RADIUS server status as Down are met.

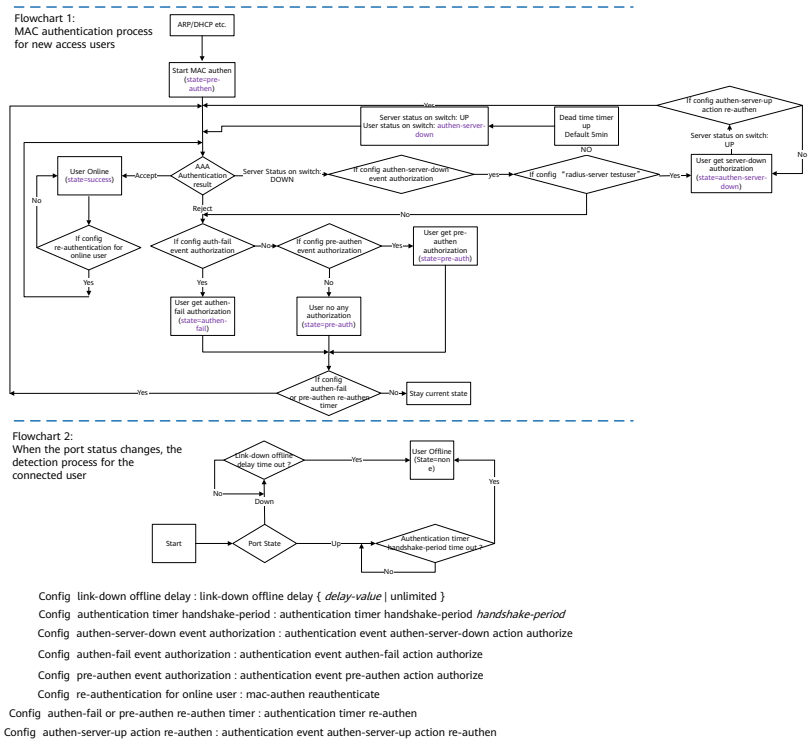
**NOTE**

If the device does not record any communication interruption in the second detection interval, the first communication interruption record is cleared.

3. When the device sends an Access-Request packet to the server for the (2n+1)th time, it marks the server status as Down.
   - If the device receives a response packet from the server, the server status reverts to Up.
   - If no response packet is received from the server and the number of packet retransmission times is not reached, the device sends an Access-Request packet to the server for the (2n+2)th time. If the server still does not respond, the device no longer sends any Access-Request packet to the server.

If multiple servers are configured in the RADIUS server template, the overall status detection time is related to the number of servers and the server selection algorithm. If a user terminal uses the client software for authentication and the timeout period of the terminal client software is less than the summary of all the status detection time, the terminal client software may dial up repeatedly and cannot access the network. If the user escape function is configured, the summary of all the status detection time must be less than the timeout period of the terminal client software to ensure that escape rights can be added to the users.

**Figure 1-11** Logic flowchart for marking the RADIUS server status as Down




The following table lists the related commands.

| Command | Description |
| --- | --- |
| **radius-server** { **dead-interval** *dead-interval* \| **dead-count** *dead-count* } | Configures conditions for marking the RADIUS server status as Down during the RADIUS server status detection.<br>• **dead-interval** *dead-interval*: Specifies the detection interval. The default value is 5 seconds.<br>• **dead-count** *dead-count*: Specifies the maximum number of consecutive unacknowledged packets. The default value is 2. |

## Automatic Detection

After the RADIUS server status is marked as Down, you can configure the automatic detection function to test the RADIUS server reachability.

Then, if the device does not receive any RADIUS Access-Request packet from users within the automatic detection interval, the device does not use the RADIUS server in this interval and the server status marked by the device is not the latest. In this case, the device sends a RADIUS Access-Request packet to the RADIUS server to verify the server status.

The automatic detection function needs to be manually enabled. The automatic server status detection function can be enabled only if the user name and password for automatic detection are configured in the RADIUS server template view on the device rather than on the RADIUS server. Authentication success is not mandatory. If the device can receive the authentication failure response packet, the RADIUS server is properly working and the device marks the RADIUS server status as Up. If the device cannot receive the response packet, the RADIUS server is unavailable and the device marks the RADIUS server status as Down.

The following table lists commands related to automatic detection.

| Command | Description |
| --- | --- |
| **radius-server testuser username** *user-name* **password cipher** *password* | Enables the automatic detection function.<br>• *user-name*: Specifies the user name for automatic detection.<br>• *password*: Specifies the password for automatic detection. |
| **radius-server detect-server interval** *interval* | Specifies the automatic detection interval. The default value is 60 seconds. |

 Copyright © Huawei Technologies Co., Ltd. 

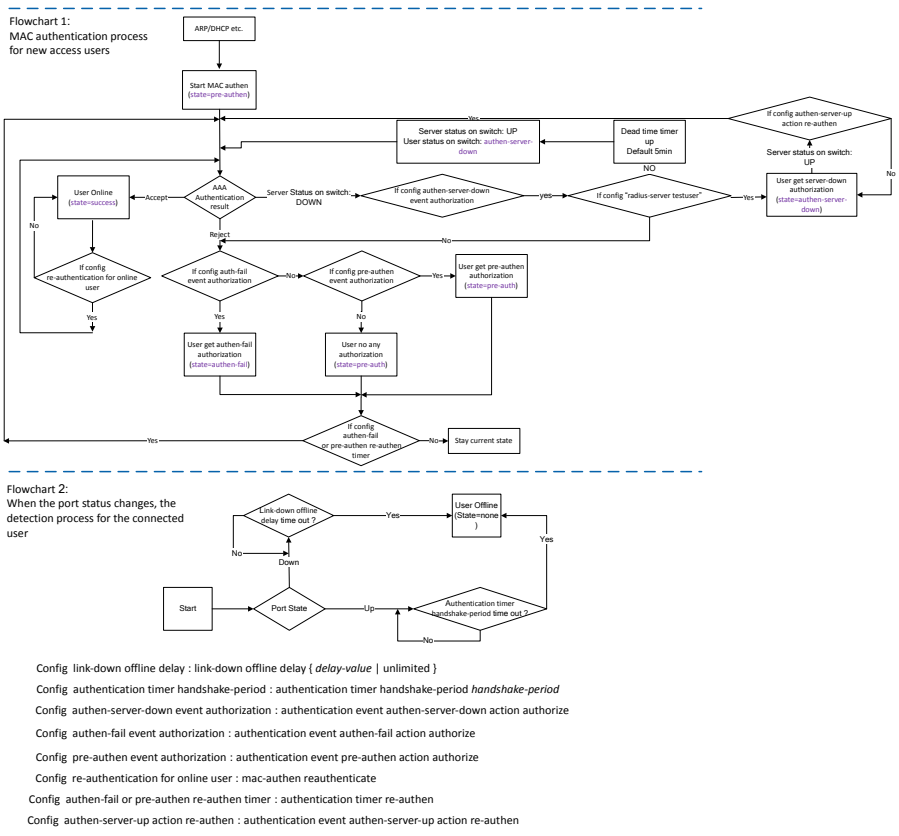
## Consecutive Processing After the RADIUS Server Status Is Marked as Down

After the device marks the RADIUS server status as Down, you can configure the escape function to make users obtain escape authorization. After the device detects that the RADIUS server status reverts to Up, you can configure the reauthentication function to make users obtain authorization from the server through reauthentication, as shown in **Figure 1-12**.

**NOTE**

For 802.1X authenticated users and MAC address authenticated users, after the RADIUS server status reverts to Up, users exist from escape authorization and are reauthenticated. For Portal authenticated users, after the RADIUS server status reverts to Up, users obtain pre-connection authorization and can be redirected to the Portal server for authentication only if the users attempt to access network resources.

**Figure 1-12** Consecutive processing after the RADIUS server status is marked as Down




The following table lists the commands for configuring the escape rights upon transition of the RADIUS server status to Down and configuring the reauthentication function, respectively.

| Command | Description |
| --- | --- |
| **authentication event authen-server-down action authorize** { **vlan** *vlan-id* \| **service-scheme** *service-scheme-name* } [ **response-fail** ] | Configures the escape function upon transition of the RADIUS server status to Down. |
| **authentication event authen-server-up action re-authen** | Configures the reauthentication function for users in escape status when the RADIUS server status reverts to Up. |

## 1.2.4.7 RADIUS CoA/DM

The device supports the RADIUS Change of Authorization (CoA) and Disconnect Message (DM) functions. CoA provides a mechanism to change the rights of online users, and DM provides a mechanism to forcibly disconnect users. This section contains the following contents:

- **RADIUS CoA/DM packet**
- **Exchange Procedure**
- **Session Flag**
- **Error Code Description**

### RADIUS CoA/DM packet

**Table 1-7** describes types of the CoA/DM packets.

**Table 1-7** RADIUS CoA/DM packet

| Packet Name | Description |
| --- | --- |
| CoA-Request | When an administrator needs to modify the rights of an online user (for example, prohibit the user from accessing a website), the RADIUS server sends this packet to the RADIUS client, requesting the client to modify the user rights. |
| CoA-ACK | If the RADIUS client successfully modifies the user rights, it returns this packet to the RADIUS server. |
| CoA-NAK | If the RADIUS client fails to modify the user rights, it returns this packet to the RADIUS server. |
| DM-Request | When an administrator needs to disconnect a user, the server sends this packet to the RADIUS client, requesting the client to disconnect the user. |
| DM-ACK | If the RADIUS client has disconnected the user, it returns this packet to the RADIUS server. |

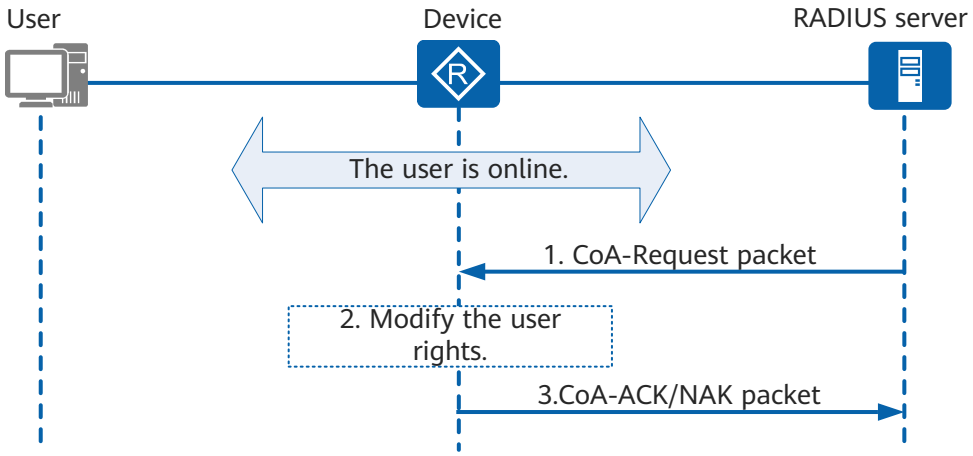
 Copyright © Huawei Technologies Co., Ltd. 

| Packet Name | Description |
| --- | --- |
| DM-NAK | If the RADIUS client fails to disconnect the user, it returns this packet to the RADIUS server. |

## Exchange Procedure

CoA allows the administrator to change the rights of an online user or perform reauthentication for the user through RADIUS after the user passes authentication. **Figure 1-13** shows the CoA interaction process.

**Figure 1-13** CoA interaction process

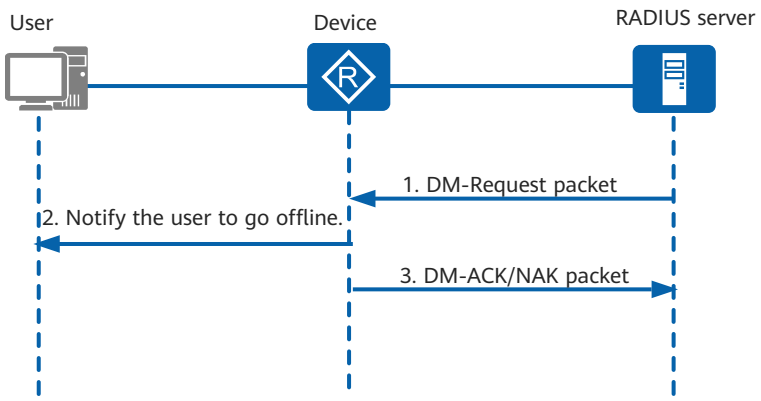



1. The RADIUS server sends a CoA-Request packet to the device according to service information, requesting the device to modify user authorization information. This packet can contain authorization information including the ACL.
2. Upon receiving the CoA-Request packet, the device performs a match check between the packet and user information on the device to identify the user. If the match succeeds, the device modifies authorization information of the user. Otherwise, the device retains the original authorization information of the user.
3. The device returns a CoA-ACK or CoA-NAK packet as follows:
   - If authorization information is successfully modified, the device sends a CoA-ACK packet to the RADIUS server.
   - If authorization information fails to be modified, the device sends a CoA-NAK packet to the RADIUS server.

When a user needs to be disconnected forcibly, the RADIUS server sends a DM packet to the device. **Figure 1-14** shows the DM interaction process.


Copyright © Huawei Technologies Co., Ltd.

**Figure 1-14** DM interaction process




1. The administrator forcibly disconnects a user on the RADIUS server. The RADIUS server sends a DM-Request packet to the device, requesting the device to disconnect the user.
2. Upon receiving the DM-Request packet, the device performs a match check between the packet and user information on the device to identify the user. If the match succeeds, the user is notified to go offline. Otherwise, the user remains online.
3. The device returns a DM-ACK or DM-NAK packet as follows:
   - If the user successfully goes offline, the device sends a DM-ACK packet to the RADIUS server.
   - Otherwise, the device sends a DM-NAK packet to the RADIUS server.

Different from the process in which authorization is performed for an online user or a user proactively goes offline, the server sends a request packet and the device sends a response packet in the CoA/DM process. If CoA/DM succeeds, the device returns an ACK packet. Otherwise, the device returns a NAK packet.

## Session Identification

Each service provided by the NAS to a user constitutes a session, with the beginning of the session defined as the point where service is first provided and the end of the session defined as the point where service is ended.

After the device receives a CoA-Request or DM-Request packet from the RADIUS server, it identifies the user depending on some RADIUS attributes in the packet. The following RADIUS attributes can be used to identify users:

- User-Name (IETF attribute #1)
- Acct-Session-ID (IETF attribute #4)
- Framed-IP-Address (IETF attribute #8)
- Calling-Station-Id (IETF attribute #31)

The match methods are as follows:

- **any** method

  The device performs a match check between an attribute and user information on the device. The priority for identifying the RADIUS attributes

 Copyright © Huawei Technologies Co., Ltd. 

used by the users is as follows: Acct-Session-ID (4) > Calling-Station-Id (31) > Framed-IP-Address (8). The device searches for the attributes in the request packet based on the priority, and performs a match check between the first found attribute and user information on the device. If the attribute is successfully matched, the device responds with an ACK packet; otherwise, the device responds with a NAK packet.

- **all** method

  The device performs a match check between all attributes and user information on the device. The device identifies the following RADIUS attributes used by the users: Acct-Session-ID (4), Calling-Station-Id (31), Framed-IP-Address (8), and User-Name (1). The device performs a match check between all the preceding attributes in the Request packet and user information on the device. If all the preceding attributes are successfully matched, the device responds with an ACK packet; otherwise, the device responds with a NAK packet.

## Error Code Description

When the CoA-Request or DM-Request packet from the RADIUS server fails to match user information on the device, the device describes the failure cause using the error code in the CoA-NAK or DM-NAK packet. For the error code description, see **Table 1-8** and **Table 1-9**.

**Table 1-8** Error codes in a CoA-NAK packet

| Name | Value | Description |
| --- | --- | --- |
| RD_DM_ERRCODE_MISSING_ATTRIBUTE | 402 | The request packet lacks key attributes, so that the integrity check of the RADIUS attributes fails. |
| RD_DM_ERRCODE_NAS_IDENTIFICATION_MISMATCH | 403 | One or more attributes in the request packet fail to be matched. |
| RD_DM_ERRCODE_INVALID_REQUEST | 404 | Parsing the attributes in the request packet fails. |

 Copyright © Huawei Technologies Co., Ltd. 

| Name | Value | Description |
| --- | --- | --- |
| RD_DM_ERRCODE_INVALID_ATTRIBUTE_VALUE | 407 | The request packet contains attributes that are not supported by the device or do not exist, so that the attribute check fails.<br>Contents of the authorization check include VLAN, ACL, CAR, number of the ACL used for redirection, and whether Huawei RADIUS extended attributes RD_hw_URL_Flag and RD_hw_Portal_URL can be authorized to the interface-based authenticated user.<br>Errors that may occur are as follows:<br>● The authorized service scheme does not exist.<br>● The authorized QoS profile does not exist or no user queue is configured in the QoS profile.<br>● The authorized values of upstream and downstream priorities exceed the maximum values.<br>● The authorized index value of the UCL group is not within the specification.<br>● The ISP VLAN and outbound interface information are incorrectly parsed.<br>● Reauthentication attributes and other attributes are authorized simultaneously. |
| RD_DM_ERRCODE_SESSION_CONTEXT_NOT_FOUND | 503 | The session request fails. The cause includes:<br>● Authorization for the current request user is being processed.<br>● The temporary RADIUS table fails to be requested.<br>● User information does not match or no user is found.<br>● The user is a non-RADIUS authentication user. |
| RD_DM_ERRCODE_RESOURCES_UNAVAILABLE | 506 | This error code is used for other authorization failures. |

**Table 1-9** Error codes in a DM-NAK packet

| Name | Value | Description |
| --- | --- | --- |
| RD_DM_ERRCODE_INVALID_REQUEST | 404 | Parsing the attributes in the request packet fails. |

 Copyright © Huawei Technologies Co., Ltd. 

| Name | Value | Description |
| --- | --- | --- |
| RD_DM_ERRCODE_SESSION_CONTEXT_NOT_REMOVABLE | 504 | The user fails to be deleted or the user does not exist. |

## 1.2.4.8 RADIUS Attributes

RADIUS attributes are Attribute fields in RADIUS packets, which carry dedicated authentication, authorization, and accounting information. This chapter covers the following sections:

- **Standard RADIUS Attributes**
- **Huawei Proprietary RADIUS Attributes**
- **Huawei-supported Extended RADIUS Attributes of Other Vendors**
- **RADIUS Attributes Available in Packets**

## Standard RADIUS Attributes

RFC2865, RFC2866, and RFC3576 define standard RADIUS attributes that are supported by all mainstream vendors. For details, see **Table 1-10**.

**Table 1-10** Standard RADIUS attributes

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 1 | User-Name | string | User name for authentication. The user name format can be *user name@domain name*, or just *user name*. |
| 2 | User-Password | string | User password for authentication, which is only valid for the Password Authentication Protocol (PAP). |
| 3 | CHAP-Password | string | Response value provided by a PPP Challenge-Handshake Authentication Protocol (CHAP) user in response to the challenge. |
| 4 | NAS-IP-Address | ipaddr | Internet Protocol (IP) address of the NAS carried in authentication request packets. By default, the attribute value is the source IP address of the authentication request packets sent by the NAS. You can change the attribute value to the specified IP address on the NAS or the IP address of the AP using the **radius-attribute nas-ip** { *ip-address* \| **ap-info** } command. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 5 | NAS-Port | integer | Physical port number of the network access server that is authenticating the user, which is in either of the following formats:<br>● new: slot ID (8 bits) + sub-slot ID (4 bits) + port number (8 bits) + Virtual Local Area Network (VLAN) ID (12 bits)<br>● old: slot ID (12 bits) + port number (8 bits) + VLAN ID (12 bits)<br>● The ADSL access physical port is in the format: slot ID (4 bits) + sub-slot ID (2 bits) + port number (2 bits) + VPI (8 bits) + VCI (16 bits). |
| 6 | Service-Type | integer | Service type of the user to be authenticated:<br>● 2 (Framed): PPP or 802.1X access users<br>● 6 (Administrative): administrator<br>● 8 (Authenticate Only): reauthentication only<br>● 10 (Call Check): MAC address authentication user or MAC address bypass authentication user |
| 7 | Framed-Protocol | integer | Encapsulation protocol of Frame services:<br>● For a non-management user, the value is fixed as 1.<br>● For a management user, the value is fixed as 6. |
| 8 | Framed-IP-Address | ipaddr | User IP address. |
| 9 | Framed-IP-Netmask | ipaddr | User IP address mask. This field must be used with the **Framed-IP-Address** field. |
| 11 | Filter-Id | string | User group name or IPv4 Access Control List (ACL) ID.<br>**NOTE**<br>● When this attribute carries the IPv4 ACL ID, the IPv4 ACL IDs must range from 3000 to 3999 (wired users) or 3000 to 3031 (wireless users).<br>● A RADIUS packet cannot carry the user group name or IPv4 ACL ID simultaneously. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 12 | Framed-MTU | integer | Maximum transmission unit (MTU) of the data link between NAS and Server. For example, in 802.1X Extensible Authentication Protocol (EAP) authentication, the NAS specifies the maximum length of the EAP packet in this attribute. An EAP packet larger than the link MTU may be lost. |
| 14 | Login-IP-Host | ipaddr | Management user IP address:<br>● If the value is 0 or 0xFFFFFFFF, the IP address of management user is not checked.<br>● If this attribute uses other values, the NAS checks whether the management user IP address is the same as the delivered attribute value. |
| 15 | Login-Service | integer | Service to use to connect the user to the login host:<br>● 0: Telnet<br>● 5: X25-PAD<br>● 50: SSH<br>● 51: FTP<br>● 52: Terminal<br>**NOTE**<br>An attribute can contain multiple service types. |
| 18 | Reply-Message | string | This attribute determines whether a user is authenticated:<br>● When an Access-Accept packet is returned, the user is successfully authenticated.<br>● When an Access-Reject packet is returned, the user fails authentication. |
| 19 | Callback-Number | string | Information sent from the authentication server and to be displayed to a user, such as a mobile number. |
| 22 | Framed-Route | string | Routing information provided by the RADIUS server to users, in format Destination/Mask NextHop Metric, for example, 192.168.1.0/24 192.168.1.1 1.<br>If the NextHop value is 0.0.0.0, the user IP address is used as the next hop address. The device can obtain only one Metric value. If the attribute delivered by the RADIUS server contains multiple Metric values, the device obtains only the first one.<br>**NOTE**<br>Currently, this Framed-Route attribute cannot provide routing information for PPPoE users on the device. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 24 | State | string | This Attribute is available to be sent by the server to the client in an Access-Challenge and MUST be sent unmodified from the client to the server in the new Access-Request reply to that challenge, if any. |
| 25 | Class | string | If the RADIUS server sends a RADIUS Access-Accept packet carrying the Class attribute to the NAS, the subsequent RADIUS Accounting-Request packets sent from the NAS must carry the Class attribute with the same value. |
| 26 | Vendor-Specific | string | Vendor-specific attribute. For details, see **Table 1-11**. A packet can carry one or more private attributes. Each private attribute contains one or more sub-attributes. |
| 27 | Session-Timeout | integer | In the Access-Request packet, this attribute indicates the maximum number of seconds a user should be allowed to remain connected.<br>In the Access-Challenge packet, this attribute indicates the duration for which EAP authentication users are reauthenticated.<br>When the value of this attribute is 0:<br>• If the **aaa-author session-timeout invalid-value enable** command is not configured, the session-timeout attribute delivered by the server does not take effect and the period for disconnecting or reauthenticating users depends on the device configuration.<br>• If the **aaa-author session-timeout invalid-value enable** command is configured, the session-timeout attribute delivered by the server takes effect and the device does not disconnect or reauthenticate users.<br>**NOTE**<br>This attribute is only valid for 802.1X, MAC address, Portal, and PPPoE authentication users.<br>When the RADIUS server delivers only this attribute, the value of attribute 29 **Termination-Action** is set to 0 (users are forced offline) by default. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 28 | Idle-Timeout | integer | Maximum number of consecutive seconds of idle connection the user is allowed before termination of the session or prompt.<br>**NOTE**<br>• This attribute is only valid for administrators, PPPoE users, and Portal users.<br>• This attribute can be used together with the traffic and direction configured using the **idle-cut** command in the service scheme view. When no authorization service scheme is configured or this command is not configured in the service scheme, and a user does not produce upstream traffic within the idle-cut period, the user is disconnected.<br>• In V200R010C00 and later versions, idle-cut is performed in seconds. In versions earlier than V200R010C00, idle-cut is performed in minutes. When a switch or an AC interconnects with an AP running a version earlier than V200R009C00, the idle-cut period is round up to an integer in seconds; for example, 60s is round up to 1 minute, and values 61s to 119s are round up to 2 minutes. |
| 29 | Termination-Action | integer | What action the NAS should take when the specified service is completed:<br>• 0: forcible disconnection<br>• 1: reauthentication<br>**NOTE**<br>This attribute is only valid for 802.1X and MAC address authentication users.<br>When the RADIUS server delivers only this attribute, the value of attribute 27 Session-Timeout is set to 3600s (for 802.1X authentication users) or 1800s (for MAC address authentication users) by default. |
| 30 | Called-Station-Id | string | Identification number of the NAS.<br>• For wired users, it is the NAS MAC address.<br>• For wireless users, it is the SSID and MAC address of the AP. |
| 31 | Calling-Station-Id | string | This Attribute allows the NAS to send in the Access-Request packet the phone number that the call came from, using Automatic Number Identification (ANI) or similar technology. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 32 | NAS-Identifier | string | String identifying the network access server originating the Access-Request. By default, the attribute value is the host name of the device. You can change the attribute value to the VLAN ID of the user or the MAC address of the AP using the **radius-server nas-identifier-format** { **hostname** \| **vlan-id** \| **ap-info** } command. |
| 40 | Acct-Status-Type | integer | Accounting-Request type:<br>● 1: Accounting-Start packet<br>● 2: Accounting-Stop packet<br>● 3: Interim-Accounting packet |
| 41 | Acct-Delay-Time | integer | Number of seconds the client has been trying to send the accounting packet (excluding the network transmission time). |
| 44 | Acct-Session-Id | string | Accounting session ID. The Accounting-Start, Interim-Accounting, and Accounting-Stop packets of the same accounting session must have the same session ID.<br>The format of this attribute is: Host name (7 bits) + Slot ID (2 bits) + Subcard number (1 bit) + Port number (2 bits) + Outer VLAN ID (4 bits) + Inner VLAN ID (5 bits) + Central Processing Unit (CPU) Tick (6 bits) + User ID prefix (2 bits) + User ID (5 bits). |
| 45 | Acct-Authentic | integer | User authentication mode:<br>● 1: RADIUS authentication<br>● 2: Local authentication<br>● 3: Other remote authentications |
| 46 | Acct-Session-Time | integer | How long (in seconds) the user has received service.<br>**NOTE**<br>If the administrator modifies the system time after the user goes online, the online time calculated by the device may be incorrect. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 49 | Acct-Terminate-Cause | string | Cause of a terminated session:<br>• User-Request (1): The user requests termination of service.<br>• Lost Carrier (2): The connection is torn down due to a handshake failure or heartbeat timeout, such as an ARP probe failure or PPP handshake failure.<br>• Lost Service (3): The connection initiated by the peer device is torn down.<br>• Idle Timeout (4): The idle timer expires.<br>• Session Timeout (5): The session times out or the traffic threshold is reached.<br>• Admin Reset (6): The administrator forces the user to go offline.<br>• Admin Reboot (7): The administrator restarts the NAS.<br>• Port Error (8): A port fails.<br>• NAS Error (9): The NAS encounters an internal error.<br>• NAS Request (10): The NAS ends the session due to resource changes.<br>• NAS Reboot (11): The NAS automatically restarts.<br>• Port Unneeded (12): The port is Down.<br>• Port Preempted (13): The port is preempted.<br>• Port Suspended (14): The port is suspended.<br>• Service Unavailable (15): The service is unavailable.<br>• Callback (16): NAS is terminating the current session to perform a callback for a new session.<br>• User Error (17): User authentication fails or times out.<br>• Host Request (18): A host sends a request. |
| 50 | Acct-Multi-Session-Id | string | Accounting ID, which is used in multi-link session scenarios. |
| 60 | CHAP-Challenge | string | Challenge field in CHAP authentication. This field is generated by the NAS for Message Digest algorithm 5 (MD5) calculation. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 61 | NAS-Port-Type | integer | NAS port type. The attribute value can be configured in the interface view. By default, the type is Ethernet (15). |
| 64 | Tunnel-Type | integer | Protocol type of the tunnel. The value is fixed as 13, indicating VLAN. |
| 65 | Tunnel-Medium-Type | integer | Medium type used on the tunnel. The value is fixed as 6, indicating Ethernet. |
| 66 | Tunnel-Client-Endpoint | string | Tunnel client address. |
| 67 | Tunnel-Server-Endpoint | string | Tunnel server address. |
| 79 | EAP-Message | string | Encapsulates Extended Access Protocol (EAP) packets so that RADIUS supports EAP authentication. When an EAP packet is longer than 253 bytes, the packet is encapsulated into multiple attributes. A RADIUS packet can carry multiple EAP-Message attributes. |
| 80 | Message-Authenticator | string | Authenticates and verifies authentication packets to prevent spoofing packets. |
| 81 | Tunnel-Private-Group-ID | string | Tunnel private group ID, which is used to deliver user VLAN IDs.<br>**NOTE**<br>To make the VLAN authorization function take effect, ensure the correct access control mode is configured:<br>• When the link type is hybrid in untagged mode, the access control mode can be MAC address or interface.<br>• When the link type is access or trunk, the access control mode can only be interface. |
| 82 | Tunnel-Assignment-Id | string | Specific ID assigned to the tunnel. |
| 85 | Acct-Interim-Interval | integer | Interim accounting interval. The value ranges from 60 to 3932100, in seconds. It is recommended that the interval be at least 600 seconds. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 87 | NAS-Port-Id | string | Port of the NAS that is authenticating the user. The NAS-Port-Id attribute has the following formats:<br>• New:<br>For Ethernet access users, the NAS-Port-Id is in the format "slot=xx; subslot=xx; port=xxx; VLAN ID=xxxx", in which "slot" ranges from 0 to 15, "subslot" 0 to 15, "port" 0 to 255, and "VLAN ID" 1 to 4094.<br>For ADSL access users, the NAS-Port-Id is in the format "slot=xx; subslot=x; port=x; VPI=xxx; VCI=xxxxx", in which "slot" ranges from 0 to 15, "subslot" 0 to 9, "port" 0 to 9, "VPI" 0 to 255, and "VCI" 0 to 65535.<br>• Old:<br>For Ethernet access users, the NAS-Port-Id is in the format "port number (2 characters) + sub-slot ID (2 bytes) + card number (3 bytes) + VLAN ID (9 characters)."<br>For ADSL access users: port number (2 characters) + sub-slot ID (2 bytes) + card number (3 bytes) + VPI (8 characters) + VCI (16 characters). The fields are prefixed with 0s if they contain fewer bytes than specified.<br>• Vendor 9: Uses the default format of Cisco for encapsulation. |
| 88 | Framed-Pool | string | Address pool, which is only included in the Access-Accept packet. It is used as authorization information in Efficient VPN. |
| 90 | Tunnel-Client-Auth-Id | string | Client tunnel ID used for authentication during tunnel setup. |
| 91 | Tunnel-Server-Auth-Id | string | Server tunnel ID used for authentication during tunnel setup. |
| 95 | NAS-IPv6-Address | ipaddr | IPv6 address carried in the authentication request packet sent by the NAS. Both the NAS-IPv6-Address and NAS-IP-Address fields can be included in a packet. |
| 195 | HW-Security Str | string | Security information of users in EAP relay authentication. |

 Copyright © Huawei Technologies Co., Ltd. 

## Huawei Proprietary RADIUS Attributes

RADIUS is a fully extensible protocol. The No. 26 attribute (Vendor-Specific) defined in RFC2865 can be used to extend RADIUS for implementing functions not supported by standard RADIUS attributes. **Table 1-11** describes Huawei proprietary RADIUS attributes.

NOTE

Extended RADIUS attributes contain the vendor ID of the device. The vendor ID of Huawei is 2011.

**Table 1-11** Huawei proprietary RADIUS attributes

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 26-1 | HW-Input-Peak-Information-Rate | integer | Peak rate at which the user accesses the NAS, in bit/s. The value is a 4-byte integer. |
| 26-2 | HW-Input-Committed-Information-Rate | integer | Average rate at which the user accesses the NAS, in bit/s. The value is a 4-byte integer. |
| 26-3 | HW-Input-Committed-Burst-Size | integer | Committed burst size (CBS) at which the user accesses the NAS, in bit/s. The value is a 4-byte integer. |
| 26-4 | HW-Output-Peak-Information-Rate | integer | Peak rate at which the NAS connects to the user, in bit/s. The value is a 4-byte integer. |
| 26-5 | HW-Output-Committed-Information-Rate | integer | Average rate at which the NAS connects to the user, in bit/s. The value is a 4-byte integer. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 26-6 | HW-Output-Committed-Burst-Size | integer | Committed burst size at which the NAS connects to the user, in bit/s. The value is a 4-byte integer. |
| 26-15 | HW-Remanent-Volume | integer | Remaining traffic. The unit is KB. |
| 26-26 | HW-Connect-ID | integer | Index of a user connection. |
| 26-28 | HW-FTP-Directory | string | Initial directory of an FTP user. |
| 26-29 | HW-Exec-Privilege | integer | Management user (such as Telnet user) priority, ranging from 0 to 15. The priority that is greater than or equal to 16 is ineffective. |
| 26-31 | HW-Qos-Data | string | Name of the QoS profile. The maximum length of the name is 31 bytes. The RADIUS server uses this field to deliver the QoS profile. The QoS profile must exist on the device. |
| 26-59 | HW-NAS-Startup-Time-Stamp | integer | NAS start time, represented by the number of seconds elapsed since 00:00:00 of January 1, 1970. |
| 26-60 | HW-IP-Host-Address | string | User IP address and MAC address carried in authentication and accounting packets, in the format A.B.C.D hh:hh:hh:hh:hh:hh. The IP address and MAC address are separated by a space.<br>If the user's IP address is detected to be invalid during authentication, the IP address is set to 255.255.255.255. |
| 26-75 | HW-Primary-WINS | ipaddr | Primary WINS server address delivered by the RADIUS server after a user is successfully authenticated. |
| 26-76 | HW-Second-WINS | ipaddr | Secondary WINS server address delivered by the RADIUS server after a user is successfully authenticated. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Attribute Name | Attribute Type | Description |
|---|---|---|---|
| 26-77 | HW-Input-Peak-Burst-Size | integer | Upstream peak rate, in bit/s. |
| 26-78 | HW-Output-Peak-Burst-Size | integer | Downstream peak rate, in bit/s. |
| 26-94 | HW-VPN-Instance | string | VPN instance name delivered by the RADIUS server after a user is successfully authenticated. It specifies the VPN to which the user belongs. |
| 26-135 | HW-Client-Primary-DNS | ipaddr | Primary DNS address delivered by the RADIUS server after a user is successfully authenticated. |
| 26-136 | HW-Client-Secondary-DNS | ipaddr | Secondary DNS address delivered by the RADIUS server after a user is successfully authenticated. |
| 26-138 | HW-Domain-Name | string | Name of the domain used for user authentication. This attribute can be the domain name contained in a user name or the name of a forcible domain. |
| 26-141 | HW-AP-Information | string | AP's MAC address used for STA authentication. |
| 26-142 | HW-User-Information | string | User security check information delivered by the RADIUS server to an Extensible Authentication Protocol over LAN (EAPoL) user to notify the user of items that require security checks. |
| 26-146 | HW-Service-Scheme | string | Service scheme name. A service scheme contains user authorization information and policies. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 26-153 | HW-Access-Type | integer | User access type carried in the authentication and accounting request packets sent by the RADIUS client to the RADIUS server:<br>● 1: Dot1x user<br>● 2: MAC address authentication user or MAC address bypass authentication<br>● 3: Portal authentication user<br>● 4: Static user<br>● 6: Management user<br>● 7: PPP users |
| 26-155 | HW-URL-Flag | integer | This attribute specifies whether a Uniform Resource Locator (URL) is forcibly pushed to users when it is used with another attribute, for example, HW-Portal-URL:<br>● 0: No<br>● 1: Yes |
| 26-156 | HW-Portal-URL | string | Forcibly pushed URL.<br>If information delivered by the RADIUS server matches the configured URL template, the URL configured in the template is used. Otherwise, the character string delivered by the RADIUS server is used. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 26-201 | HW-User-Extend-Info | string | Extended user information. This attribute is contained in authentication and accounting request packets. A packet can contain multiple **HW-User-Extend-Info** attributes. The following describes extended user information:<br>● User-Position: Service code of the location where a user goes online<br>● User-Position-Type: Type of the location where a user goes online<br>● AP-Device-Code: AP code<br>● AP-POS-X: Longitude of a moving AP<br>● AP-POS-Y: Latitude of a moving AP<br>● Wifi-Density: Field strength<br>● HW-Access-Time: user access time. The value is the number of seconds elapsed since 00:00:00 of January 1, 1970.802.1X authentication supports only this field.<br>● wan-src-ip: Source IPv4/IPv6 address of the external network<br>An IPv4 address is expressed by an unsigned integer in host byte order, for example, 2880036141. An IPv6 address is expressed by a colon-delimited hexadecimal notation string (XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX), for example, CDCD:910A:2222:5498:1111:3900:2020:6328.<br>● wan-src-start-port: Start source IPv4/IPv6 port numbers of the external network<br>A source port can be a TCP or an IP port, and the port number range is from 0 to 65535. If only one port is available, the start and end port numbers are the same.<br>● wan-src-end-port: End source IPv4/IPv6 port numbers of the external network<br>A source port can be a TCP or an IP port, and the port number range is from 0 to 65535.<br>This attribute applies only to MAC address authentication and Portal authentication. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 26-237 | HW-Web-Authen-Info | string | Information sent from the portal server via the device (which transparently transmits the information) to the RADIUS server. For example, a user selects the authentication-free option and time information for next login, based on which the RADIUS server saves the MAC address of the user for a period of time. Upon the next login of the user, the login page is not displayed. Instead, MAC address authentication is preferentially used. This attribute can be used for transparent transmission in complex modes such as EAP. |
| 26-241 | HW-User-Addr-Network | ipaddr | User's address segment. |
| 26-242 | HW-DNS-Domain-Name | string | DNS domain name. |
| 26-243 | HW-Auto-Update-URL | string | URL address for version upgrade. |
| 26-244 | HW-Reachable-Detect | string | Server reachability detection information. Authentication packets carrying this attribute are server detection packets. |
| 26-247 | HW-Tariff-Input-Octets | string | Number of upstream bytes at the specified tariff level sent to the accounting server. This field is included in the accounting packets. The unit can be byte, kilobyte, megabyte, or gigabyte. The format is *Tariff level*:*Number of upstream bytes*. An accounting packet can contain the traffic of at most 8 tariff levels. |
| 26-248 | HW-Tariff-Output-Octets | string | Number of downstream bytes at the specified tariff level sent to the accounting server. This field is included in the accounting packets. The unit can be byte, kilobyte, megabyte, or gigabyte. The format is *Tariff level*:*Number of downstream bytes*. An accounting packet can contain the traffic of at most 8 tariff levels. |
| 26-249 | HW-Tariff-Input-Gigawords | string | Number of times larger the number of upstream bytes at the specified tariff level is than 4G. This field and the **HW-Tariff-Input-Octets** field specify the number of upstream bytes at the specified tariff level. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| 26-250 | HW-Tariff-Output-Gigawords | string | Number of times larger the number of downstream bytes at the specified tariff level is than 4G. This field and the **HW-Tariff-Output-Octets** field specify the number of downstream bytes at the specified tariff level. |
| 26-254 | HW-Version | string | Software version of the device. |
| 26-255 | HW-Product-ID | string | NAS product name. |

## Huawei-supported Extended RADIUS Attributes of Other Vendors

Huawei devices support some extended RADIUS attributes of Microsoft. For details, see **Table 1-12**.

**Table 1-12** Huawei-supported extended RADIUS attributes of other vendors

| Attribute No. | Attribute Name | Attribute Type | Description |
| --- | --- | --- | --- |
| MICROSOFT-16 | MS-MPPE-Send-Key | string | This attribute indicates the MPPE sending key. |
| MICROSOFT-17 | MS-MPPE-Recv-Key | string | This attribute indicates the MPPE receiving key. |

## RADIUS Attributes Available in Packets

Different RADIUS packets carry different RADIUS attributes.

- For the RADIUS attributes available in authentication packets, see **Table 1-13**.
- For the RADIUS attributes available in accounting packets, see **Table 1-14**.
- For the RADIUS attributes available in authorization packets, see **Table 1-15**.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

The following describes the values in the tables:

- 1: indicates that the attribute must appear once in the packet.
- 0: indicates that the attribute cannot appear in the packet (it will be discarded if it is contained).
- 0-1: indicates that the attribute can appear once or does not appear in the packet.
- 0+: indicates that the attribute may appear multiple times or does not appear in the packet.

**Table 1-13** RADIUS attributes available in authentication packets

| Attribute No. | Access-Request | Access-Accept | Access-Reject | Access-Challenge |
|---|---|---|---|---|
| User-Name(1) | 1 | 0-1 | 0 | 0 |
| User-Password(2) | 0-1 | 0 | 0 | 0 |
| CHAP-Password(3) | 0-1 | 0 | 0 | 0 |
| NAS-IP-Address(4) | 1 | 0 | 0 | 0 |
| NAS-Port(5) | 1 | 0 | 0 | 0 |
| Service-Type(6) | 1 | 0-1 | 0 | 0 |
| Framed-Protocol(7) | 1 | 0-1 | 0 | 0 |
| Framed-IP-Address(8) | 0-1 | 0-1 | 0 | 0 |
| Framed-IP-Netmask(9) | 0 | 0-1 | 0 | 0 |
| Filter-Id(11) | 0 | 0-1 | 0 | 0 |
| Framed-Mtu(12) | 0-1 | 0 | 0 | 0 |
| Login-IP-Host(14) | 0-1 | 0-1 | 0 | 0 |
| Login-Service(15) | 0 | 0-1 | 0 | 0 |
| Reply-Message(18) | 0 | 0-1 | 0-1 | 0-1 |
| Callback-Number(19) | 0 | 0-1 | 0 | 0 |
| Framed-Route(22) | 0 | 0-1 | 0 | 0 |
| State(24) | 0-1 | 0-1 | 0 | 0-1 |
| Class(25) | 0 | 0-1 | 0 | 0 |
| Session-Timeout(27) | 0 | 0-1 | 0-1 | 0-1 |
| Idle-Timeout(28) | 0 | 0-1 | 0 | 0 |
| Termination-Action(29) | 0 | 0-1 | 0 | 0-1 |
| Called-Station-Id(30) | 0-1 | 0 | 0 | 0 |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Access-Request | Access-Accept | Access-Reject | Access-Challenge |
|---|---|---|---|---|
| Calling-Station-Id(31) | 1 | 0-1 | 0 | 0 |
| NAS-Identifier(32) | 1 | 0 | 0 | 0 |
| Acct-Session-id(44) | 1 | 0 | 0 | 0 |
| CHAP-Challenge(60) | 0-1 | 0 | 0 | 0 |
| NAS-Port-Type(61) | 1 | 0 | 0 | 0 |
| Tunnel-Type(64) | 0 | 0-1 | 0 | 0 |
| Tunnel-Medium-Type(65) | 0 | 0-1 | 0 | 0 |
| Tunnel-Client-Endpoint(66) | 0-1 | 0-1 | 0 | 0 |
| Tunnel-Server-Endpoint(67) | 0-1 | 0-1 | 0 | 0 |
| EAP-Message(79) | 0-1 | 0-1 | 0-1 | 0-1 |
| Message-Authenticator(80) | 0-1 | 0-1 | 0-1 | 0-1 |
| Tunnel-Private-Group-ID(81) | 0 | 0-1 | 0-1 | 0 |
| Tunnel-Assignment-Id(82) | 0 | 0-1 | 0 | 0 |
| Acct-Interim-Interval(85) | 0 | 0-1 | 0 | 0 |
| NAS-Port-Id(87) | 0-1 | 0 | 0 | 0 |
| Framed-Pool(88) | 0 | 1 | 0 | 0 |
| Tunnel-Client-Auth-Id(90) | 0 | 0-1 | 0 | 0 |
| Tunnel-Server-Auth-Id(91) | 0 | 0-1 | 0 | 0 |
| NAS-IPv6-Address(95) | 0-1 | 0 | 0 | 0 |
| HW-SecurityStr(195) | 0-1 | 0 | 0 | 0 |
| HW-Input-Peak-Information-Rate(26-1) | 0 | 0-1 | 0 | 0 |
| HW-Input-Committed-Information-Rate(26-2) | 0 | 0-1 | 0 | 0 |
| HW-Input-Committed-Burst-Size(26-3) | 0 | 0-1 | 0 | 0 |


Copyright © Huawei Technologies Co., Ltd.

| Attribute No. | Access-Request | Access-Accept | Access-Reject | Access-Challenge |
| --- | --- | --- | --- | --- |
| HW-Output-Peak-Information-Rate(26-4) | 0 | 0-1 | 0 | 0 |
| HW-Output-Committed-Information-Rate(26-5) | 0 | 0-1 | 0 | 0 |
| HW-Output-Committed-Burst-Size(26-6) | 0 | 0-1 | 0 | 0 |
| HW-Remanent-Volume(26-15) | 0 | 0-1 | 0 | 0 |
| HW-Connect-ID(26-26) | 1 | 0 | 0 | 0 |
| Ftp-directory(26-28) | 0 | 0-1 | 0 | 0 |
| HW-Exec-Privilege(26-29) | 0 | 0-1 | 0 | 0 |
| HW-Qos-Data(26-31) | 0 | 0-1 | 0 | 0 |
| HW-NAS-Startup-Time-Stamp(26-59) | 1 | 0 | 0 | 0 |
| HW-IP-Host-Address(26-60) | 1 | 0 | 0 | 0 |
| HW-Primary-WINS(26-75) | 0 | 0-1 | 0 | 0 |
| HW-Second-WINS(26-76) | 0 | 0-1 | 0 | 0 |
| HW-Input-Peak-Burst-Size(26-77) | 0 | 0-1 | 0 | 0 |
| HW-Output-Peak-Burst-Size(26-78) | 0 | 0-1 | 0 | 0 |
| HW-VPN-Instance(26-94) | 0 | 0-1 | 0 | 0 |
| HW-Client-Primary-DNS(26-135) | 0 | 0-1 | 0 | 0 |
| HW-Client-Secondary-DNS(26-136) | 0 | 0-1 | 0 | 0 |
| HW-Domain-Name(26-138) | 1 | 0 | 0 | 0 |
| HW-AP-Information(26-141) | 1 | 0 | 0 | 0 |
| HW-User-Information(26-142) | 0 | 0-1 | 0 | 0 |
| HW-Web-Proxy-Name(26-143) | 0 | 0-1 | 0 | 0 |


Copyright © Huawei Technologies Co., Ltd.

| Attribute No. | Access-Request | Access-Accept | Access-Reject | Access-Challenge |
|---|---|---|---|---|
| HW-Port-Forward-Name(26-144) | 0 | 0-1 | 0 | 0 |
| HW-IP-Forwarding-Name(26-145) | 0 | 0-1 | 0 | 0 |
| HW-Service-Scheme(26-146) | 0 | 0-1 | 0 | 0 |
| HW-Access-Type(26-153) | 1 | 0-1 | 0 | 0 |
| HW-User-Extend-Info(26-201) | 0-1 | 0 | 0 | 0 |
| HW-Web-Authen-Info(26-237) | 1 | 0 | 0 | 0 |
| HW-User-Addr-Network(26-241) | 0 | 0-1 | 0 | 0 |
| HW-DNS-Domain-Name(26-242) | 0 | 0-1 | 0 | 0 |
| HW-Auto-Update-URL(26-243) | 0 | 0-1 | 0 | 0 |
| HW-Reachable-Detect(26-244) | 0 | 0 | 0 | 0 |
| HW-Version(26-254) | 1 | 0 | 0 | 0 |
| HW-Product-ID(26-255) | 1 | 0 | 0 | 0 |
| MS-MPPE-Send-Key(MICROSOFT-16) | 0 | 0-1 | 0 | 0 |
| MS-MPPE-Recv-Key(MICROSOFT-17) | 0 | 0-1 | 0 | 0 |

**Table 1-14** RADIUS attributes available in accounting packets

| Attribute No. | Accounting-Request (Start) | Accounting-Request (Interim-Update) | Accounting-Request (Stop) | Accounting-Response (start) | Accounting-Response (Interim-Update) | Accounting-Response (Stop) |
|---|---|---|---|---|---|---|
| User-Name(1) | 1 | 1 | 1 | 0 | 0 | 0 |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Accounting-Request (Start) | Accounting-Request (Interim-Update) | Accounting-Request (Stop) | Accounting-Response (start) | Accounting-Response (Interim-Update) | Accounting-Response (Stop) |
|---|---|---|---|---|---|---|
| NAS-IP-Address(4) | 1 | 1 | 1 | 0 | 0 | 0 |
| NAS-Port(5) | 1 | 1 | 1 | 0 | 0 | 0 |
| Service-Type(6) | 1 | 1 | 1 | 0 | 0 | 0 |
| Framed-Protocol(7) | 1 | 1 | 1 | 0 | 0 | 0 |
| Framed-IP-Address(8) | 1 | 1 | 1 | 0 | 0 | 0 |
| Class(25) | 0-1 | 0-1 | 0-1 | 0 | 0 | 0 |
| Session-Timeout(27) | 0 | 0 | 0 | 0-1 | 0-1 | 0 |
| Called-Station-Id(30)<br>**NOTE**<br>For users who access the network through PPP authentication, this attribute is optional. If the authentication request packet does not carry this attribute, then neither does the accounting request packet. | 1 | 1 | 1 | 0 | 0 | 0 |
| Calling-Station-Id(31) | 1 | 1 | 1 | 0 | 0 | 0 |
| NAS-Identifier(32) | 1 | 1 | 1 | 0 | 0 | 0 |
| Acct-Status-Type(40) | 1 | 1 | 1 | 0 | 0 | 0 |
| Acct-Delay-Time(41) | 0-1 | 1 | 1 | 0 | 0 | 0 |
| Acct-Output-Octets(43) | 0-1 | 0-1 | 0-1 | 0 | 0 | 0 |
| Acct-Session-Id(44) | 1 | 1 | 1 | 0 | 0 | 0 |
| Acct-Authentic(45) | 1 | 1 | 1 | 0 | 0 | 0 |
| Acct-Session-Time(46) | 0 | 1 | 1 | 0 | 0 | 0 |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Accounting-Request (Start) | Accounting-Request (Interim-Update) | Accounting-Request (Stop) | Accounting-Response (start) | Accounting-Response (Interim-Update) | Accounting-Response (Stop) |
|---|---|---|---|---|---|---|
| Acct-Terminate-Cause(49) | 0 | 0 | 1 | 0 | 0 | 0 |
| Acct-Multi-Session-Id (50) | 0-1 | 0-1 | 0-1 | 0 | 0 | 0 |
| Event-Timestamp(55) | 1 | 1 | 1 | 0 | 0 | 0 |
| NAS-Port-Type(61) | 1 | 1 | 1 | 0 | 0 | 0 |
| Tunnel-Client-Endpoint(66) | 0-1 | 0-1 | 0-1 | 0 | 0 | 0 |
| Tunnel-Server-Endpoint(67) | 0-1 | 0-1 | 0-1 | 0 | 0 | 0 |
| Tunnel-Assignment-Id(82) | 0-1 | 0-1 | 0-1 | 0 | 0 | 0 |
| NAS-Port-Id(87) | 1 | 1 | 1 | 0 | 0 | 0 |
| Tunnel-Client-Auth-Id(90) | 0-1 | 0-1 | 0-1 | 0 | 0 | 0 |
| Tunnel-Server-Auth-Id(91) | 0-1 | 0-1 | 0-1 | 0 | 0 | 0 |
| NAS-IPv6-Address(95) | 0-1 | 0-1 | 0-1 | 0 | 0 | 0 |
| HW-Input-Committed-Information-Rate(26-2) | 1 | 1 | 1 | 0 | 0 | 0 |
| HW-Output-Committed-Information-Rate(26-5) | 1 | 1 | 1 | 0 | 0 | 0 |
| HW-Connect-ID(26-26) | 1 | 1 | 1 | 0 | 0 | 0 |
| HW-IP-Host-Address(26-60) | 1 | 1 | 1 | 0 | 0 | 0 |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | Accounting-Request (Start) | Accounting-Request (Interim-Update) | Accounting-Request (Stop) | Accounting-Response (start) | Accounting-Response (Interim-Update) | Accounting-Response (Stop) |
|---|---|---|---|---|---|---|
| HW-Domain-Name(26-138) | 1 | 1 | 1 | 0 | 0 | 0 |
| HW-AP-Information(26-141) | 0-1 | 0-1 | 0-1 | 0 | 0 | 0 |
| HW-User-Information(26-142) | 0 | 0 | 0 | 0-1 | 0-1 | 0 |
| HW-Access-Type(26-153) | 0-1 | 0-1 | 0-1 | 0 | 0 | 0 |
| HW-User-Extend-Info(26-201) | 0-1 | 0-1 | 0-1 | 0 | 0 | 0 |
| HW-Reachable-Detect(26-244) | 0 | 0 | 0 | 0 | 0 | 0 |
| HW-Tariff-Input-Octets(26-247) | 0 | 0-1 | 0-1 | 0 | 0 | 0 |
| HW-Tariff-Output-Octets(26-248) | 0 | 0-1 | 0-1 | 0 | 0 | 0 |
| HW-Tariff-Input-Gigawords(26-249) | 0 | 0-1 | 0-1 | 0 | 0 | 0 |
| HW-Tariff-Output-Gigawords(26-250) | 0 | 0-1 | 0-1 | 0 | 0 | 0 |
| MS-MPPE-Send-Key(MICROSOFT-16) | 0 | 0 | 0 | 0 | 0 | 0 |
| MS-MPPE-Recv-Key(MICROSOFT-17) | 0 | 0 | 0 | 0 | 0 | 0 |

**Table 1-15** RADIUS attributes available in CoA/DM packets

| Attribute No. | CoA REQUEST | CoA ACK | CoA NAK | DM REQUEST | DM ACK | DM NAK |
|---|---|---|---|---|---|---|
| User-Name(1) | 0-1 | 0-1 | 0-1 | 0-1 | 0-1 | 0-1 |
| NAS-IP-Address(4) | 0-1 | 0-1 | 0-1 | 0-1 | 0-1 | 0-1 |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | CoA REQUEST | CoA ACK | CoA NAK | DM REQUEST | DM ACK | DM NAK |
|---|---|---|---|---|---|---|
| NAS-Port(5) | 0-1 | 0 | 0 | 0-1 | 0 | 0 |
| Framed-IP-Address(8) | 0-1 | 0-1 | 0-1 | 0-1 | 0-1 | 0-1 |
| Filter-Id(11) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| Session-Timeout(27) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| Idle-Timeout(28) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| Termination-Action(29) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| Calling-Station-Id(31) | 0-1 | 0-1 | 0-1 | 0-1 | 0-1 | 0-1 |
| NAS-Identifier(32) | 0 | 0-1 | 0-1 | 0 | 0 | 0 |
| Acct-Session-Id(44) | 1 | 1 | 1 | 1 | 1 | 1 |
| Tunnel-Type(64) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| Tunnel-Medium-Type(65) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| Tunnel-Private-Group-ID(81) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| Acct-Interim-Interval(85) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| NAS-Port-Id(87) | 0-1 | 0 | 0 | 0-1 | 0 | 0 |
| HW-Input-Peak-Information-Rate(26-1) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| HW-Input-Committed-Information-Rate(26-2) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| HW-Output-Peak-Information-Rate(26-4) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| HW-Output-Committed-Information-Rate(26-5) | 0-1 | 0 | 0 | 0 | 0 | 0 |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute No. | CoA REQUEST | CoA ACK | CoA NAK | DM REQUEST | DM ACK | DM NAK |
|---|---|---|---|---|---|---|
| HW-Output-Committed-Burst-Size(26-6) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| HW-Qos-Data(26-31) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| HW-Input-Peak-Burst-Size(26-77) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| HW-Output-Peak-Burst-Size(26-78) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| HW-Service-Scheme(26-146) | 0-1 | 0 | 0 | 0 | 0 | 0 |
| MS-MPPE-Send-Key(MICROSOFT-16) | 0 | 0 | 0 | 0 | 0 | 0 |
| MS-MPPE-Recv-Key(MICROSOFT-17) | 0 | 0 | 0 | 0 | 0 | 0 |

### 1.2.4.9 RADIUS Attribute Disablement and Translation

Different vendors support different collections of RADIUS attributes and each vendor may have their private attributes. As a result, RADIUS attributes of different vendors may be incompatible and RADIUS attributes sent between devices from different vendors fail to be parsed. To resolve this issue, the RADIUS attribute disablement and translation functions are often used in interconnection and replacement scenarios.

#### RADIUS Attribute Disablement

The RADIUS server may have RADIUS attributes with the same attribute IDs and names as but different encapsulation formats or contents from those on the device. In this case, you can configure the RADIUS attribute disablement function to disable such attributes. The device then does not parse these attributes after receiving them from the RADIUS server, and does not encapsulate these attributes into RADIUS packets to be sent to the server.

Currently, Huawei-supported RADIUS attributes (with Huawei-supported attribute names and IDs) in a sent or received packet can be disabled on a device.

#### RADIUS Attribute Translation

RADIUS attribute translation is used for achieve compatibility between RADIUS attributes defined by different vendors. For example, a Huawei device delivers the priority of an administrator using the Huawei proprietary attribute Exec-Privilege (26-29), whereas another vendor's NAS and the RADIUS server deliver this priority

 Copyright © Huawei Technologies Co., Ltd. 

using the Login-service(15) attribute. In a scenario where the Huawei device and another vendor's NAS share one RADIUS server, users want the Huawei device to be compatible with the Login-service(15) attribute. After RADIUS attribute translation is configured on the Huawei device, the device automatically processes the Login-service(15) attribute in a received RADIUS authentication response packet as the Exec-Privilege (26-29) attribute.

Devices translate RADIUS attributes in a sent or received packet based on the Type, Length, and Value fields of the RADIUS attributes.

- If translation between attributes A and B is configured in the transmit direction on the device and the device sends a packet containing attribute A, the Type field of the attribute is attribute B but the Value field is encapsulated based on the content and format of attribute A.
- If translation between attributes A and B is configured in the receive direction on the device and the device receives a packet containing attribute A, it parses the Value field of attribute A as that of attribute B. To be specific, it can be understood that the device receives a packet containing attribute B instead of attribute A after attribute translation is configured.

Huawei-supported and non-Huawei-supported RADIUS attributes can be translated into each other. **Table 1-16** shows the mode for translating Huawei-supported and non-Huawei-supported RADIUS attributes into each other.

NOTE

- The device can translate a RADIUS attribute of another vendor only if the length of the Type field in the attribute is 1 octet.
- The device can translate the RADIUS attribute only when the type of the source RADIUS attribute is the same as that of the destination RADIUS attribute. For example, the types of NAS-Identifier and NAS-Port-Id attributes are string, and they can be translated into each other. The types of NAS-Identifier and NAS-Port attributes are string and integer respectively, they cannot be translated into each other.

**Table 1-16** RADIUS attribute translation mode

| Whether Huawei Supports the Source RADIUS Attribute | Whether Huawei Supports the Destination RADIUS Attribute | Supported Translation Direction | Configuration Command (RADIUS Server Template View) |
|---|---|---|---|
| Supported | Supported | Transmit and receive directions | **radius-attribute translate** *src-attribute-name dest-attribute-name* { **receive** \| **send** \| **access-accept** \| **access-request** \| **account-request** \| **account-response** } * |

 Copyright © Huawei Technologies Co., Ltd. 

| Whether Huawei Supports the Source RADIUS Attribute | Whether Huawei Supports the Destination RADIUS Attribute | Supported Translation Direction | Configuration Command (RADIUS Server Template View) |
| --- | --- | --- | --- |
| Supported | Not supported | Transmit direction | **radius-attribute translate extend** *src-attribute-name* **vendor-specific** *dest-vendor-id dest-sub-id* { **access-request** \| **account-request** } * |
| Not supported | Supported | Receive direction | **radius-attribute translate extend vendor-specific** *src-vendor-id src-sub-id dest-attribute-name* { **access-accept** \| **account-response** } * |

# 1.2.5 HWTACACS AAA

## 1.2.5.1 Overview of HWTACACS

HWTACACS is an information exchange protocol that uses the client/server model to provide centralized validation of users who attempt to access your switch. It uses Transmission Control Protocol (TCP) and TCP port number 49 to transmit data. HWTACACS provides independent authentication, authorization, and accounting for users accessing the Internet through Point-to-Point Protocol (PPP) or Virtual Private Dial-up Network (VPDN) and for administrators. As an enhancement to TACACS (RFC 1492), it can be implemented on different servers.

Both HWTACACS and RADIUS have the following characteristics:

- Client/Server model
  - HWTACACS client: generally resides on the Network Access Server (NAS) and can reside on the entire network. The client is responsible for transmitting user information to the specified HWTACACS server and then performs operations accordingly based on the server-returned information.
  - HWTACACS server: generally runs on the central computer or workstation. The server maintains user authentication and network access information, and is responsible for receiving user connection requests, authenticating users, and returning required information to clients.
- Share key used for encrypting user information
- Good scalability

However, HWTACACS takes advantages over RADIUS in transmission and encryption reliability, and better suitability for security control. **Table 1-17** lists the differences between HWTACACS and RADIUS.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 1-17** Comparisons between HWTACACS and RADIUS

| Item | HWTACACS | RADIUS |
| --- | --- | --- |
| Data transmission | Uses TCP, which is more reliable. | Uses UDP, which is more efficient. |
| Encryption | Encrypts the entire body of the packet except the standard HWTACACS header. | Encrypts only the password in the packet. |
| Authentication and authorization | Separates authentication from authorization so that they can be implemented on different security servers. | Combines authentication and authorization. |
| Command line authorization | Supported. The commands that a user can use are restricted by both the command level and AAA. When a user enters a command, the command is executed only after being authorized by the HWTACACS server. | Not supported. The commands that a user can use depend on their user level. A user can only use the commands of the same level as or lower level than the user level. |
| Application | Security control. | Accounting. |

### 1.2.5.2 HWTACACS Packets

An HWTACACS client and an HWTACACS server communicate using HWTACACS packets sent over TCP/IP networks. Unlike RADIUS packets with the same format, HWTACACS packets (including **HWTACACS Authentication Packet**, **HWTACACS Authorization Packet**, and **HWTACACS Accounting Packet**) are formatted differently. HWTACACS packets all share the same **HWTACACS Packet Header**.

#### HWTACACS Packet Header

HWTACACS defines a 12-byte header that appears in all HWTACACS packets. **Figure 1-15** shows the header.


Copyright © Huawei Technologies Co., Ltd.

**Figure 1-15** HWTACACS packet header

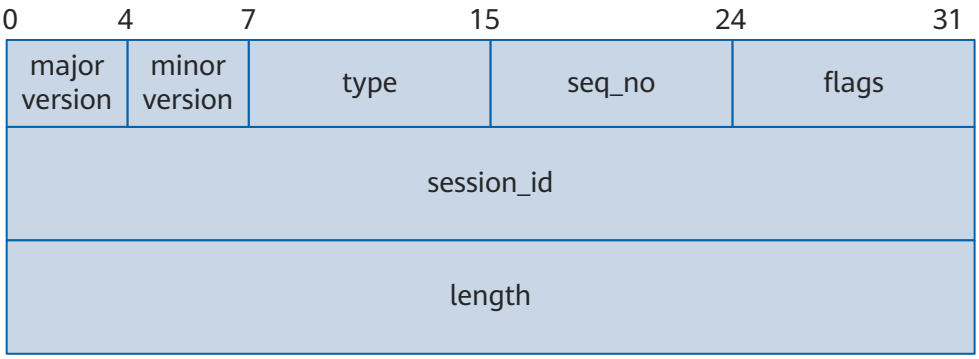



**Table 1-18** Fields in HWTACACS packet header

| Field | Description |
| --- | --- |
| major version | Major HWTACACS version number. The current version is 0xc. |
| minor version | Minor HWTACACS version number. The current version is 0x0. |
| type | HWTACACS packet type. Allowed values are:<br>• 0x01 (authentication)<br>• 0x02 (authorization)<br>• 0x03 (accounting) |
| seq_no | Sequence number of the packet in a session. The first packet in a session has the sequence number 1 and each subsequent packet increments the sequence number by 1. The value ranges from 1 to 254. |
| flags | Encryption flag on the packet body. This field contains 8 bits, of which only the first bit has a valid value. The value 0 indicates that the packet body is encrypted, and the value 1 indicates that the packet body is not encrypted. |
| session_id | ID of the HWTACACS session, which is the unique identifier of a session. |
| length | Total length of the HWTACACS packet body, excluding the packet header. |

## HWTACACS Authentication Packet Format

HWTACACS defines three types of authentication packets:


Copyright © Huawei Technologies Co., Ltd.

- **Authentication Start**: indicates the type of authentication to be performed, and contains the user name and authentication data. This packet is only sent as the first message in an HWTACACS authentication process.
- **Authentication Continue**: indicates that the authentication process has not ended. This packet is sent by a client when the client receives an Authentication Reply packet from the server.
- **Authentication Reply**: notifies the client of the current authentication status. When the server receives an Authentication Start or Authentication Continue packet from a client, the server sends this packet to the client.

The following figure shows the HWTACACS Authentication Start packet body.

**Figure 1-16** HWTACACS Authentication Start packet body

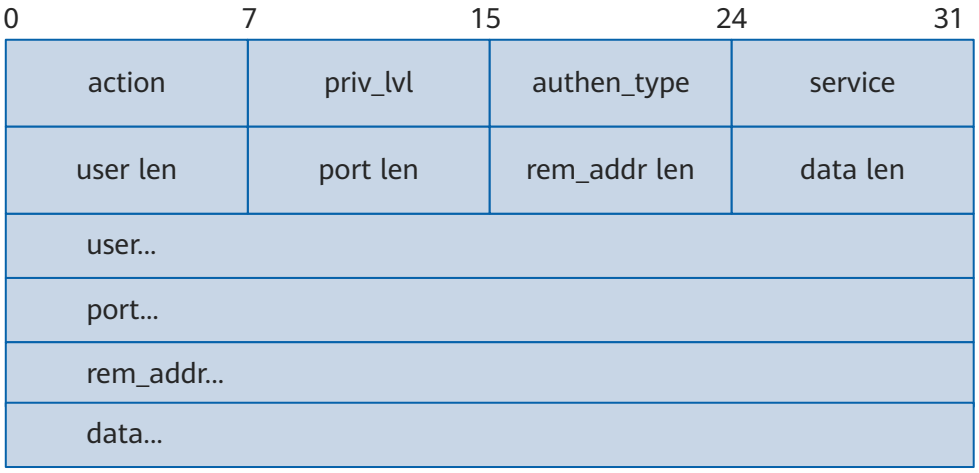



**Table 1-19** Fields in HWTACACS Authentication Start packet

| Field | Description |
| --- | --- |
| action | Authentication action to be performed. Only the login authentication (0x01) action is supported. |
| priv_lvl | Privilege level of a user. The value ranges from 0 to 15. |
| authen_type | Authentication type. Allowed values are:<br>• 0x03 (CHAP authentication)<br>• 0x02 (PAP authentication)<br>• 0x01 (ASCII authentication) |
| service | Type of the service requesting authentication. The value varies by user type:<br>• PPP users: PPP(0x03)<br>• Administrators: LOGIN(0x01)<br>• Other users: NONE(0x00) |
| user len | Length of the user name entered by a login user. |
| port len | Length of the port field. |

 Copyright © Huawei Technologies Co., Ltd. 

| Field | Description |
| --- | --- |
| rem_addr len | rem_addr field length. |
| data len | Authentication data length. |
| user | Name of the user requesting authentication. The maximum length is 129. |
| port | Name of the user interface requesting authentication. The maximum length is 47.<br>• For administrators, this field indicates the user terminal interface, such as console0 and vty1. For example, the authen_type of Telnet users is ASCII, service is LOGIN, and port is vtyx.<br>• For other users, this field indicates the user access interface. |
| rem_addr | IP address of the login user. |
| data | Authentication data. Different data is encapsulated depending on the values of action and authen_type. For example, when PAP authentication is used, the value of this field is PAP plain-text password. |

The following figure shows the HWTACACS Authentication Continue packet body.

**Figure 1-17** HWTACACS Authentication Continue packet body

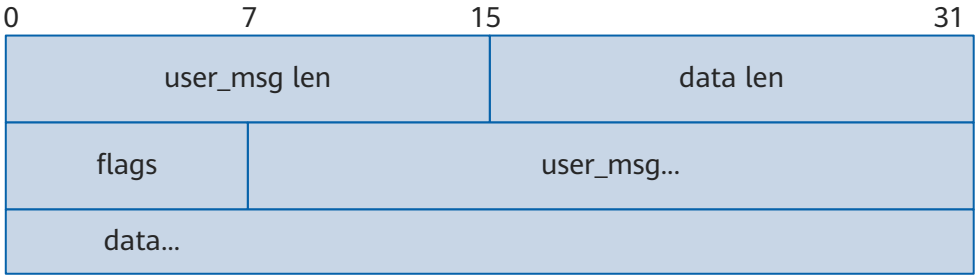



**Table 1-20** Fields in HWTACACS Authentication Continue packet

| Field | Description |
| --- | --- |
| user_msg len | Length of the character string entered by a login user. |
| data len | Authentication data length. |
| flags | Authentication continue flag. Allowed values are:<br>• 0: Authentication continues.<br>• 1: Authentication has ended. |


Copyright © Huawei Technologies Co., Ltd.

| Field | Description |
| --- | --- |
| user_msg | Character string entered by a login user. This field carries the user login password to respond to the server_msg field in the Authentication Reply packet. |
| data | Authentication data. Different data is encapsulated depending on the values of action and authen_type. For example, when PAP authentication is used, the value of this field is PAP plain-text password. |

The following figure shows the HWTACACS Authentication Reply packet body.

**Figure 1-18** HWTACACS Authentication Reply packet body

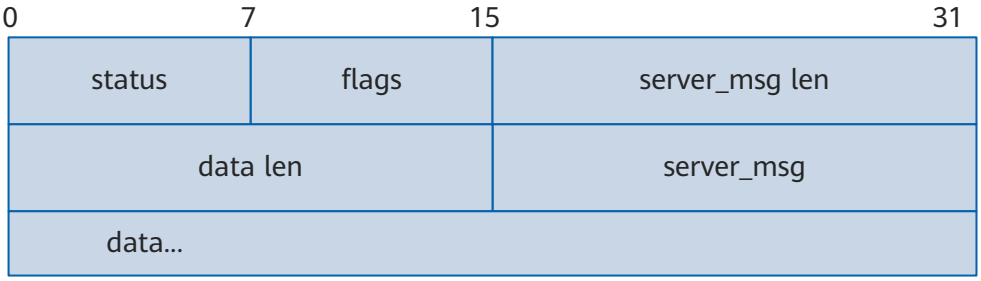



**Table 1-21** Fields in HWTACACS Authentication Reply packet

| Field | Description |
| --- | --- |
| status | Current authentication status. Allowed values are:<br>• PASS (0x01): Authentication succeeds.<br>• FAIL (0x02): Authentication fails.<br>• GETDATA (0x03): Request user information.<br>• GETUSER (0x04): Request user name.<br>• GETPASS (0x05): Request password.<br>• RESTART (0x06): Request reauthentication.<br>• ERROR (0x07): The authentication packets received by the server have errors.<br>• FOLLOW (0x21): The server requests reauthentication. |
| flags | Whether the client displays the password entered by user in plain text. The value 1 indicates that the password is not displayed in plain text. |
| server_msg len | Length of the server_msg field. |
| data len | Authentication data length. |

 Copyright © Huawei Technologies Co., Ltd. 

| Field | Description |
| --- | --- |
| server_msg | Optional field. This field is sent by the server to the user to provide additional information. |
| data | Authentication data, providing information to the client. |

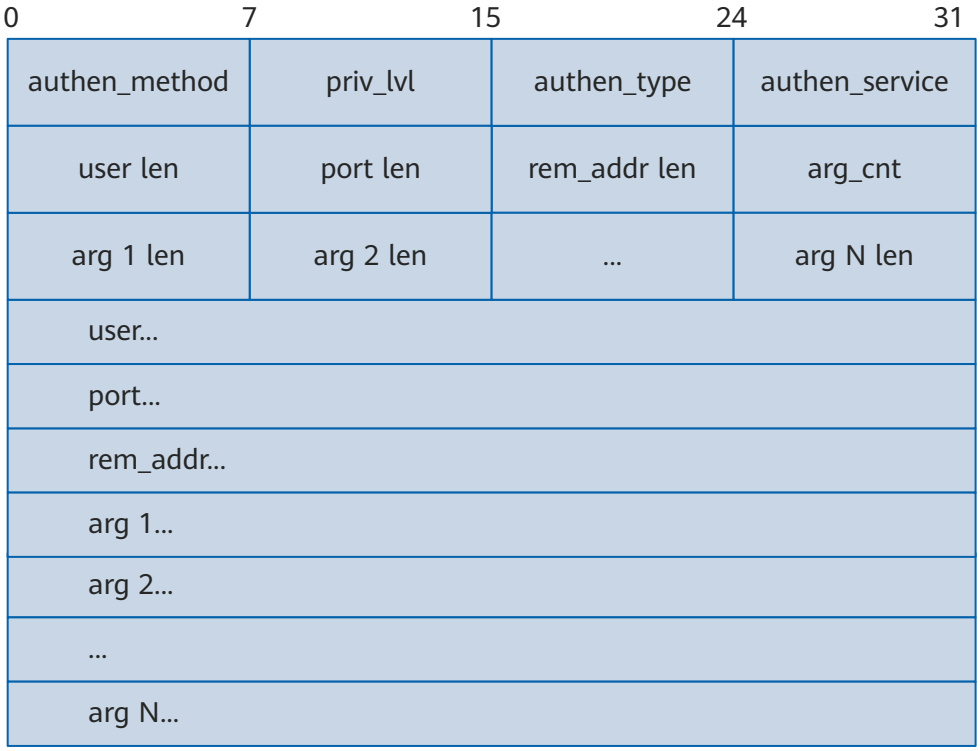
## HWTACACS Authorization Packet Format

HWTACACS defines two types of authorization packets:

- **Authorization Request**: contains a fixed set of fields that indicate how a user is authenticated or processed and a variable set of attributes that describe the information for which authorization is requested.
- **Authorization Response**: contains a variable set of attributes that can limit or change the client's action.

The following figure shows the HWTACACS Authorization Request packet body.

**Figure 1-19** HWTACACS Authorization Request packet body




**NOTE**

The meanings of the following fields in the Authorization Request packet are the same as those in the Authentication Start packet, and are not described here: priv_lvl, authen_type, authen_service, user len, port len, rem_addr len, port, and rem_addr.

 Copyright © Huawei Technologies Co., Ltd. 

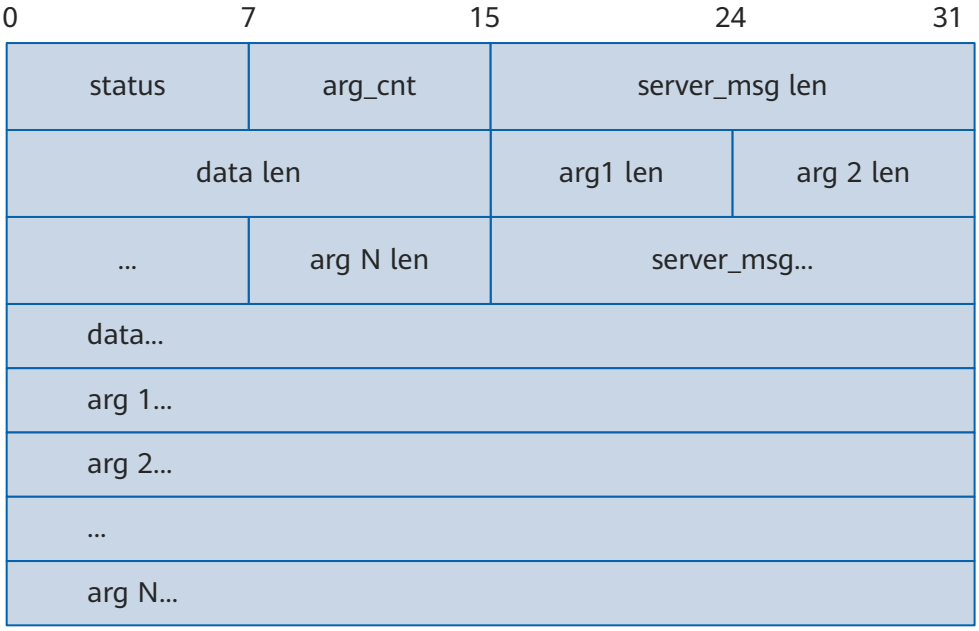
**Table 1-22** Fields in HWTACACS Authorization Request packet

| Field | Description |
| --- | --- |
| authen_method | Authentication method used by the client to acquire user information. Allowed values are:<br>● 0x00 (no authentication method configured)<br>● 0x01 (none authentication)<br>● 0x05 (local authentication)<br>● 0x06 (HWTACACS authentication)<br>● 0x10 (RADIUS authentication) |
| authen_service | Type of the service requesting authentication. The value varies by user type:<br>● PPP users: PPP(0x03)<br>● Administrators: LOGIN(0x01)<br>● Other users: NONE(0x00) |
| arg_cnt | Number of attributes carried in the Authorization Request packet. |
| argN | Attribute of the Authorization Request packet, including the following:<br>● cmd: first argument in the command for authorization request.<br>● cmd-arg: arguments in the command for authorization request. The format is fixed as cmd-arg=*command parameter*. The cmd-arg=<cr> is added at the end of the command line. The total length of cmd-arg=*command parameter* cannot exceed 255 bytes, and each command parameter cannot be longer than 247 bytes. |

The following figure shows the HWTACACS Authentication Reply packet body.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 1-20** HWTACACS Authorization Response packet body




NOTE

Meanings of the following fields are the same as those in the HWTACACS Authentication Reply packet, and are not described here: server_msg len, data len, and server_msg.

**Table 1-23** Fields in HWTACACS Authorization Response packet

| Field | Description |
| --- | --- |
| status | Authorization status. Allowed values are:<br>• 0x01 (authorization is successful)<br>• 0x02 (the attributes in Authorization Request packets are modified by the TACACS server)<br>• 0x10 (authorization fails)<br>• 0x11 (an error occurs on the authorization server)<br>• 0x21 (an authorization server is re-specified) |
| arg_cnt | Number of attributes carried in an Authorization Response packet. |
| argN | Authorization attribute delivered by the HWTACACS authorization server. |

## HWTACACS Accounting Packet Format

HWTACACS defines two types of accounting packets:

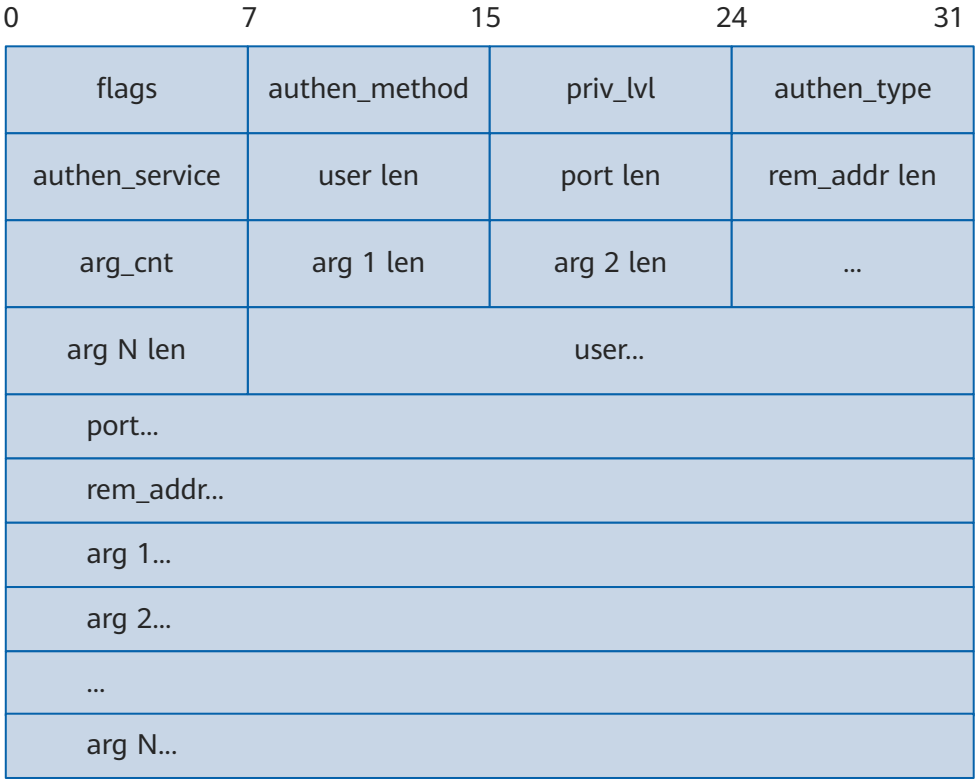
- **Accounting Request**: contains information used to provide accounting for a service provided to a user.


Copyright © Huawei Technologies Co., Ltd.

- **Accounting Response**: After receiving and recording an Accounting Request packet, the server returns this packet, indicating that accounting has been completed, and the record has been securely committed.

The following figure shows the HWTACACS Accounting Request packet body.

**Figure 1-21** HWTACACS Accounting Request packet body




**NOTE**

Meanings of the following fields in the Accounting Request packet are the same as those in the Authorization Request packet, and are not described here: authen_method, priv_lvl, authen_type, user len, port len, rem_addr len, port, and rem_addr.

**Table 1-24** Fields in HWTACACS Accounting Request packet

| Field | Description |
| --- | --- |
| flags | Accounting type. Allowed values are:<br>• 0x02 (start accounting)<br>• 0x04 (stop accounting)<br>• 0x08 (interim accounting) |


Copyright © Huawei Technologies Co., Ltd.

| Field | Description |
| --- | --- |
| authen_service | Type of the service requesting authentication, which varies by user type:<br>• PPP users: PPP(0x03)<br>• Administrators: LOGIN(0x01)<br>• Other users: NONE(0x00) |
| arg_cnt | Number of attributes carried in the Accounting Request packet. |
| argN | Attribute of the Accounting Request packet. |

The following figure shows the HWTACACS Accounting Response packet body.

**Figure 1-22** HWTACACS Accounting Response packet body

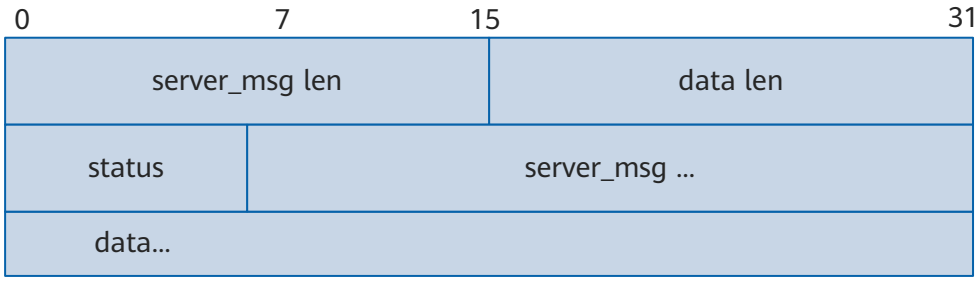



**Table 1-25** Fields in HWTACACS Accounting Response packet

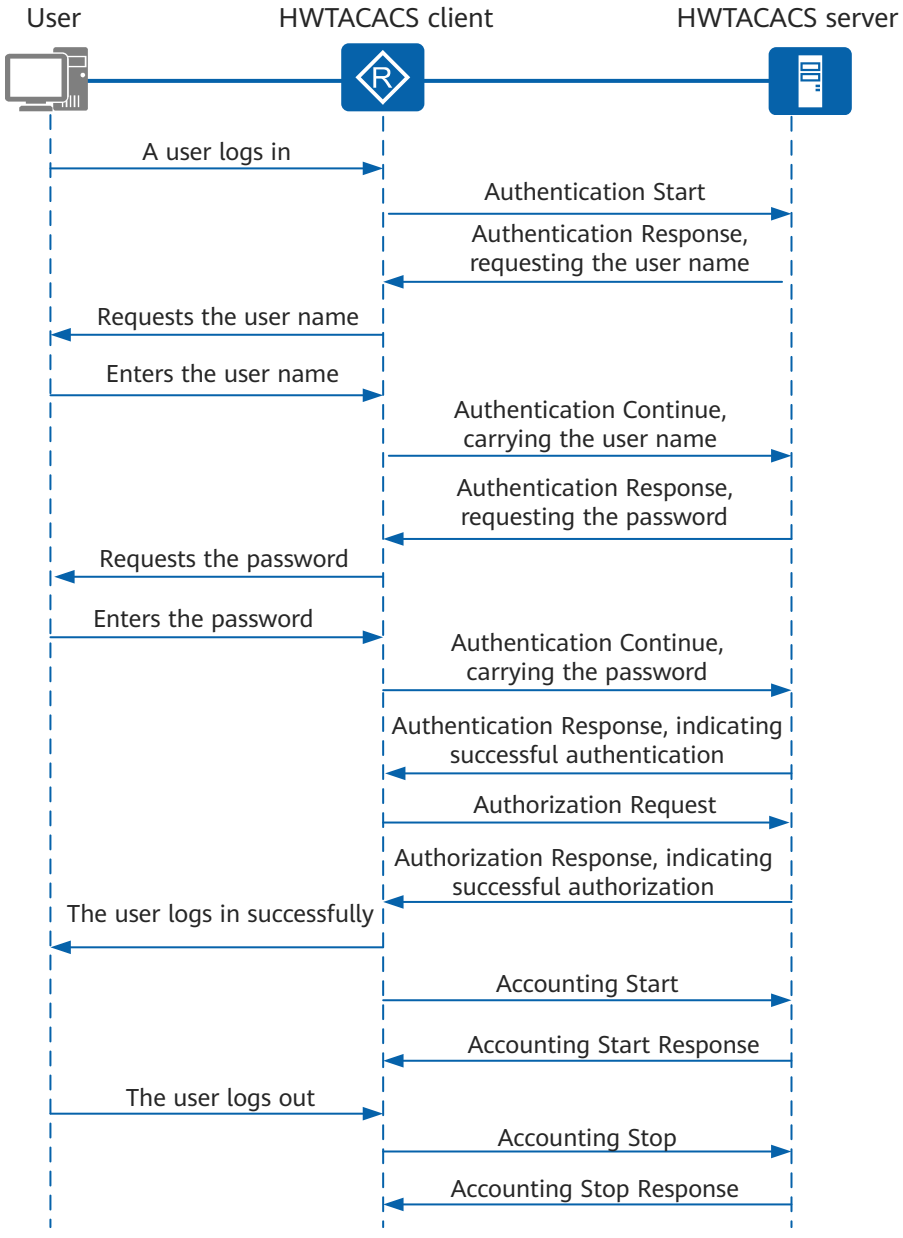
| Field | Description |
| --- | --- |
| server_msg len | Length of the server_msg field. |
| data len | Length of the data field. |
| status | Accounting status. Allowed values are:<br>• 0x01 (accounting is successful)<br>• 0x02 (accounting fails)<br>• 0x03 (no response)<br>• 0x21 (the server requests reaccounting) |
| server_msg | Information sent by the accounting server to the client. |
| data | Information sent by the accounting server to the administrator. |


Copyright © Huawei Technologies Co., Ltd.

### 1.2.5.3 HWTACACS Authentication, Authorization, and Accounting Process

This section describes how HWTACACS performs authentication, authorization, and accounting for Telnet users. **Figure 1-23** shows the message exchange process.

**Figure 1-23** HWTACACS message interaction




The following describes the HWTACACS message exchange process shown in **Figure 1-23**:

1. A Telnet user sends a request packet.
2. After receiving the request packet, the HWTACACS client sends an Authentication Start packet to the HWTACACS server.

 Copyright © Huawei Technologies Co., Ltd. 

3. The HWTACACS server sends an Authentication Response packet to request the user name.
4. After receiving the Authentication Response packet, the HWTACACS client sends a packet to query the user name.
5. The user enters the user name.
6. The HWTACACS client sends an Authentication Continue packet containing the user name to the HWTACACS server.
7. The HWTACACS server sends an Authentication Response packet to request the password.
8. After receiving the Authentication Response packet, the HWTACACS client queries the password.
9. The user enters the password.
10. The HWTACACS client sends an Authentication Continue packet containing the password to the HWTACACS server.
11. The HWTACACS server sends an Authentication Response packet, indicating that the user has been authenticated.
12. The HWTACACS client sends an Authorization Request packet to the HWTACACS server.
13. The HWTACACS server sends an Authorization Response packet, indicating that the user has been authorized.
14. The HWTACACS client receives the Authorization Response packet and displays the login page.
15. The HWTACACS client sends an Accounting Request (start) packet to the HWTACACS server.
16. The HWTACACS server sends an Accounting Response packet.
17. The user requests to go offline.
18. The HWTACACS client sends an Accounting Request (stop) packet to the HWTACACS server.
19. The HWTACACS server sends an Accounting Response packet.

NOTE

HWTACACS and TACACS+ protocols of other vendors can implement authentication, authorization, and accounting. HWTACACS is compatible with other TACACS+ protocols because their authentication procedures and implementations are the same.

## 1.2.5.4 HWTACACS Attributes

HWTACACS uses different attributes to define authorization and accounting to be performed. The attributes are carried by the argN field. This section describes HWTACACS attributes in detail.

## Overview of HWTACACS Attributes

**Table 1-26** describes the HWTACACS attributes supported by the device. The device can only parse the attributes included in the table.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 1-26** HWTACACS attributes for common use

| Attribute Name | Description |
| --- | --- |
| acl | Authorization ACL ID. |
| addr | A network address. |
| autocmd | An auto-command to run after a user logs in to the device. |
| bytes_in | Number of input bytes transmitted during this connection. K, M, and G represent KByte, MByte, and GByte. No unit is displayed if byte is used. |
| bytes_out | Number of output bytes transmitted during this connection. K, M, and G represent KByte, MByte, and GByte. No unit is displayed if byte is used. |
| callback-line | The line number to use for a callback, such as a mobile number. |
| cmd | Command name for a shell command that is to be run. The maximum length is 251 characters. The complete command is encapsulated when the command is recorded and the first keyword is encapsulated when the command is authorized. |
| cmd-arg | Parameter in the command line to be authorized. The cmd-arg=<cr> is added at the end of the command line. |
| disc_cause | Cause for a connection to be taken offline. Only Accounting-Stop packets carry this attribute. Disconnection causes include:<br>• 1 (a user requests to go offline)<br>• 2 (data forwarding is interrupted)<br>• 3 (service is interrupted)<br>• 4 (idle timeout)<br>• 5 (session timeout)<br>• 7 (the administrator requests to go offline)<br>• 9 (the NAS is faulty)<br>• 10 (the NAS requests to go offline)<br>• 12 (the port is suspended)<br>• 17 (user information is incorrect)<br>• 18 (a host requests to go offline) |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute Name | Description |
| --- | --- |
| disc_cause_ext | Extension of the disc-cause attribute to support vendor-specific causes for a connection to be taken offline. Only Accounting-Stop packets carry this attribute. Extended disconnection causes include:<br>• 1022 (unknown reason)<br>• 1020 (the EXEC terminal tears down the connection)<br>• 1022 (an online Telnet user forcibly disconnects this user)<br>• 1023 (the user cannot be switched to the SLIP/PPP client due to no remote IP address)<br>• 1042 (PPP PAP authentication fails)<br>• 1045 (PPP receives a Terminate packet from the remote end)<br>• 1046 (the upper-layer device requests the device to tear down the PPP connection)<br>• 1063 (PPP handshake fails)<br>• 1100 (session times out) |
| dnaverage | Average downstream rate, in bit/s. |
| dnpeak | Peak downstream rate, in bit/s. |
| dns-servers | IP address of the primary DNS server. |
| elapsed_time | Online duration of a user, in seconds. |
| ftpdir | Initial directory of an FTP user. |
| gw-password | Password for the gateway during the L2TP tunnel authentication. The value is a string of 1 to 248 characters. If the value contains more than 248 characters, only the first 248 characters are valid. |
| idletime | Period after which an idle session is terminated. If a user does not perform any operation within this period, the system disconnects the user. |
| l2tp-hello-interval | Interval for sending L2TP Hello packets. This attribute is currently not supported. |
| l2tp-hidden-avp | Attribute value pair (AVP) of L2TP. This attribute is currently not supported. |
| l2tp-nosession-timeout | Number of seconds that a tunnel remains active with no sessions before timeout or shutdown. This attribute is currently not supported. |
| l2tp-group-num | L2TP group number. Other L2TP attributes take effect only if this attribute is delivered. Otherwise, other L2TP attributes are ignored. |
| l2tp-tos-reflect | TOS of L2TP. The device does not support this attribute. |

 Copyright © Huawei Technologies Co., Ltd. 

| Attribute Name | Description |
| --- | --- |
| l2tp-tunnel-authen | Whether an L2TP tunnel is authenticated:<br>● 0: not authenticated<br>● 1: authenticated |
| l2tp-udp-checksum | Whether L2TP should perform UDP checksums for data packets. |
| nocallback-verify | No callback authentication is required. |
| nohangup | Whether the device automatically disconnects a user who has executed the **autocmd** command. This attribute is valid only after the **autocmd** attribute is configured. The value can be true or false:<br>● true: The user is not disconnected.<br>● false: The user is disconnected. |
| paks_in | Number of packets received by the device. |
| paks_out | Number of packets sent by the device. |
| priv-lvl | User level. |
| protocol | A protocol that is a subset of a service. It is valid only for PPP and connection services. Legal values matching service types are as follows:<br>● Connection service type: pad, telnet<br>● PPP service type: ip, vpdn<br>● Other service types: This attribute is not used. |
| task_id | Task ID. The task IDs recorded when a task starts and ends must be the same. |
| timezone | Time zone for all timestamps included in this packet. |
| tunnel-id | User name used to authenticate a tunnel in establishment. The value is a string of 1 to 29 characters. If the value contains more than 29 characters, only the first 29 characters are valid. |
| tunnel-type | Tunnel type. The device supports only L2TP tunnels. For L2TP tunnels, the value is 3. |
| service | Service type, which can be accounting or authorization. |
| source-ip | Local IP address of a tunnel. |
| upaverage | Average upstream rate, in bit/s. |
| uppeak | Peak upstream rate, in bit/s. |

 Copyright © Huawei Technologies Co., Ltd. 

## HWTACACS Attributes Available in Packets

Depending on usage scenarios, HWTACACS authorization packets can also be classified into EXEC authorization packets, command line authorization packets, and access user authorization packets. Different authorization packets carry different attributes. For details, see **Table 1-27**. The following describes the use of HWTACACS authorization packets for different usage scenarios:

- EXEC authorization packets: Used by the HWTACACS server to control rights of the management users logging in through Telnet, console port, SSH, and FTP.
- Command line authorization packets: Used by the device to authorize each command line executed by the user. Only authorized command lines can be executed.
- Access user authorization packets: Used by the HWTACACS server to control the rights of NAC users such as 802.1X and Portal users.

Depending on connection types, HWTACACS accounting packets can also be classified into network accounting packets, connection accounting packets, EXEC accounting packets, system accounting packets, and command accounting packets. Different accounting packets carry different attributes. For details, see **Table 1-28**. The following describes the use of HWTACACS accounting packets for different connection types:

- Network accounting packets: Used when networks are accessed by PPP users. For example, when a PPP user connects to a network, the server sends an accounting start packet; when the user is using network services, the server periodically sends interim accounting packets; when the user goes offline, the server sends an accounting stop packet.
- Connection accounting packets: Used when users log in to the server through Telnet or FTP clients. When a user connects to the device, the user can run commands to access a remote server and obtain files from the server. The device sends an accounting start packet when the user connects to the remote server, and an accounting stop packet when the user disconnects from the remote server.
- EXEC accounting packets: Used when users log in to the device through Telnet or FTP. When a user connects to a network, the server sends an accounting start packet; when the user is using network services, the server periodically sends interim accounting packets; when the user goes offline, the server sends an accounting stop packet.
- System accounting packets: Used during fault diagnosis. The server records system-level events to help administrators monitor the device and locate network faults.
- Command accounting packets: When an administrator runs any command on the device, the device sends the command to the HWTACACS server through a command accounting stop packet so that the server can record the operations performed by the administrator.

NOTE

- **Y**: The packet supports this attribute.
- **N**: The packet does not support this attribute.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 1-27** HWTACACS attributes available in authorization packets

| Attribute | Command Line Authorization Packet | EXEC Authorization Response Packet | Access User Authorization Response Packet |
|---|---|---|---|
| acl | N | Y | N |
| addr | N | N | Y |
| addr-pool | N | N | Y |
| autocmd | N | Y | N |
| callback-line | N | Y | Y |
| cmd | Y | N | N |
| cmd-arg | Y | N | N |
| dnaverage | N | N | Y |
| dnpeak | N | N | Y |
| dns-servers | N | N | Y |
| ftpdir | N | Y | N |
| gw-password | N | N | Y |
| idletime | N | Y | N |
| ip-addresses | N | N | Y |
| l2tp-group-num | N | N | Y |
| l2tp-tunnel-authen | N | N | Y |
| nocallback-verify | N | Y | N |
| nohangup | N | Y | N |
| priv-lvl | N | Y | N |
| source-ip | N | N | Y |
| tunnel-type | N | N | Y |
| tunnel-id | N | N | Y |
| upaverage | N | N | Y |

 Copyright © Huawei Technologies Co., Ltd. 

**Table 1-28** HWTACACS attributes available in accounting packets

| Attribute | Network Accounting Start Packet | Network Accounting Stop Packet | Network Interim Accounting Packet | Connection Accounting Start Packet | Connection Accounting Stop Packet | EXEC Accounting Start Packet | EXEC Accounting Stop Packet | EXEC Interim Accounting Packet | System Accounting Stop Packet | Command Line Accounting Stop Packet |
|---|---|---|---|---|---|---|---|---|---|---|
| addr | Y | Y | Y | Y | Y | N | N | N | N | N |
| bytes_in | N | Y | Y | N | Y | N | Y | Y | N | N |
| bytes_out | N | Y | Y | N | Y | N | Y | Y | N | N |
| cmd | N | N | N | Y | Y | N | N | N | N | Y |
| disc_cause | N | Y | N | N | N | N | Y | Y | N | N |
| disc_cause_ext | N | Y | N | N | N | N | Y | Y | N | N |
| elapsed_time | N | Y | Y | N | Y | N | Y | Y | Y | N |
| paks_in | N | Y | Y | N | Y | N | Y | Y | N | N |
| paks_out | N | Y | Y | N | Y | N | Y | Y | N | N |
| priv-lvl | N | N | N | N | N | N | N | N | N | Y |
| protocol | Y | Y | Y | Y | Y | N | N | N | N | N |
| service | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| task_id | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| timezone | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| tunnel-id | N | N | N | N | N | N | N | N | N | N |
| tunnel-type | Y | N | N | N | N | N | N | N | N | N |

# 1.2.6 HACA AAA

## 1.2.6.1 Overview of HACA

 Copyright © Huawei Technologies Co., Ltd. 

Small- and medium-sized enterprises usually have small network scales and dispersed network sites. In addition, there are a relatively small number of concurrent users. Huawei provides the Cloud Managed Network Solution, which serves small- and medium-sized enterprises utilizing the public network. This solution supports centralized multi-tenant management, plug-and-play network devices, and batch network service deployment. Compared with the architecture and deployment modes of traditional networks, this solution provides a shorter network deployment period, lower maintenance costs, and better network scalability.

Generally, the CloudCampus Solution uses Portal authentication. The authentication server is located on the cloud, so packets between the device and server must traverse a NAT device. However, Portal protocol packets cannot traverse the NAT device. HACA implements communication between the device and server, and then Portal authentication can be performed. Only a Huawei Agile Controller server can be used as an HACA server.

HACA is based on the mobile Internet protocol HTTP/2.

- HACA supports Portal authentication or MAC address-prioritized Portal authentication.
- HACA does not support administrative access, IPsec, SSL VPN, IP session, PPPoE, L2TP, VM, 802.1X, and independent MAC address authentication.
- HACA does not support wired user access.

### 1.2.6.2 HACA Packets

Service packets record messages exchanged between devices and the HACA server. The following table describes service packet types specified by the **msgType** field.

**Table 1-29** HACA service packet type

| Service Packet Type | msgType | Description |
| --- | --- | --- |
| Registration request packet | 1 | After setting up an HTTP/2 persistent connection with an HACA server, a device sends this packet to the HACA server to register device information. |
| Registration response packet | 2 | The HACA server sends this packet to the device, indicating that a persistent connection has been set up successfully and they can exchange service packets. |
| Authentication request packet | 3 | The device sends this packet to the HACA server. The HACA server determines whether to permit the access based on user information carried in this packet. |

 Copyright © Huawei Technologies Co., Ltd. 

| Service Packet Type | msgType | Description |
| --- | --- | --- |
| Authentication response packet | 4 | The HACA server sends an authentication response packet to the device. If all attributes in the authentication request packet are acceptable, the server considers that the user passes the authentication and sends this packet. After receiving this packet, the device grants network access rights to the user. |
| Proactive authorization request packet | 6 | The HACA server sends this packet to the device after the user passes authentication. |
| Proactive authorization response packet | 5 | The device sends this packet to the HACA server and modifies user rights. |
| Accounting-start request packet | 7 | The device sends this packet to the HACA server when the user starts to access network resources. |
| Accounting response packet | 8 | After receiving and recording an accounting-start request packet, the HACA server returns an accounting response packet. |
| Logout notification packet | 9 | If the HACA server logs out the user, the device sends a logout notification packet and the HACA server does not need to reply. If accounting has been performed for the user, the packet carries accounting information. |
| Logout request packet | 11 | If the device triggers user logout, it sends a logout request packet to the HACA server. If the HACA server triggers user logout, it sends this packet to notify the device that a specified user has logged out. |
| Logout response packet | 12 | If the device triggers user logout, the HACA server sends a logout response packet to the device. If the HACA server triggers user logout, the device sends a logout response packet to the HACA server and releases the related authorization entry. |
| User synchronization request packet | 13 | User information can be periodically synchronized between the HACA server and device to ensure user information consistency. Either the device or the HACA server sends a user synchronization request packet to trigger user information synchronization. |

 Copyright © Huawei Technologies Co., Ltd. 

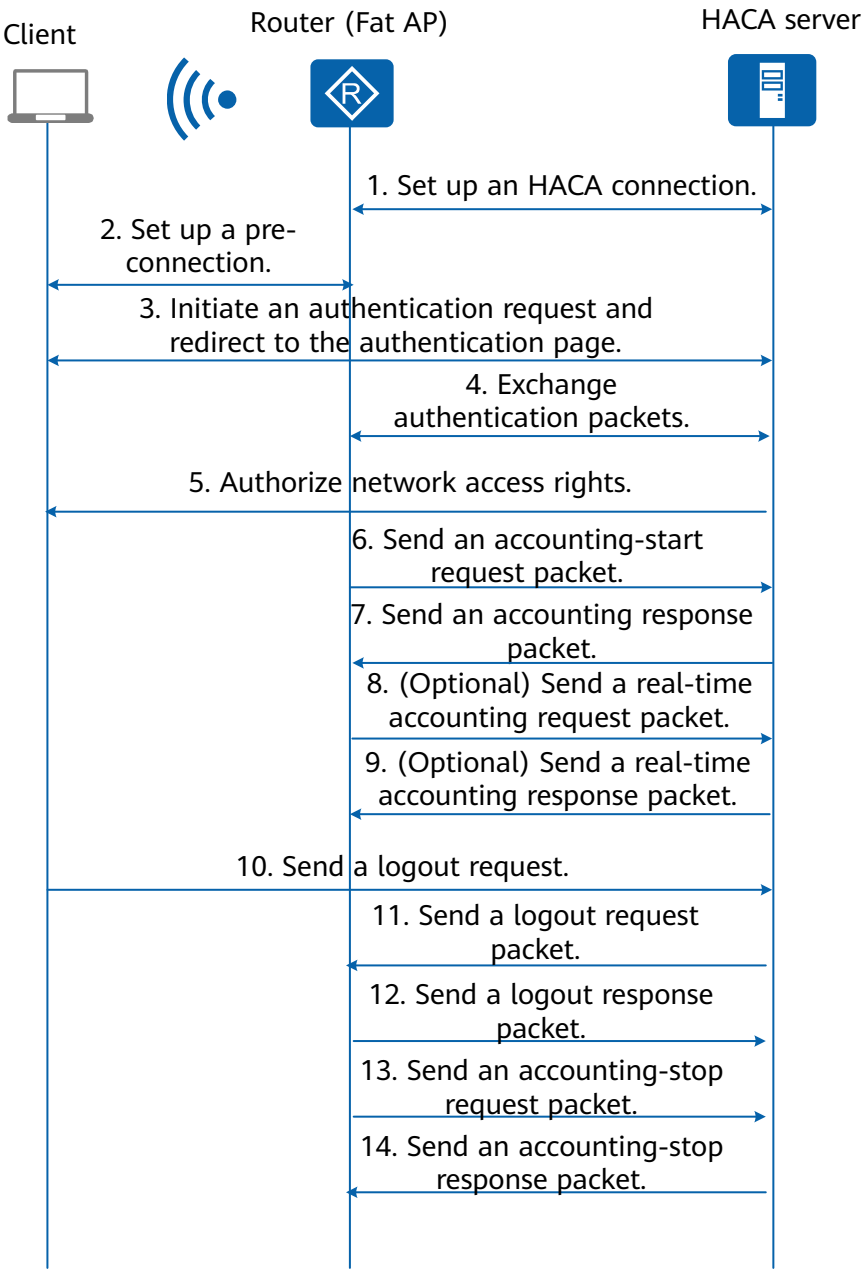
| Service Packet Type | msgType | Description |
| --- | --- | --- |
| User synchronization response packet | 14 | When the device or HACA server triggers user information synchronization, the peer end returns a user synchronization response packet. |
| CoA-Request packet | 16 | When an administrator needs to modify the rights of an online user (for example, prohibit the user from accessing a website), the HACA server sends this packet to the device, requesting the device to modify the user rights. |
| CoA-Response packet | 15 | If the device successfully modifies the user rights, it sends this packet to the HACA server. |

### 1.2.6.3 HACA Authentication, Authorization, and Accounting Process

HACA only supports MAC address-prioritized Portal authentication. The Agile Controller server deployed on the cloud acts as an external Portal server and an HACA server to provide authentication and accounting services. A router acts as a Fat AP to provide wireless access. It also acts as an authentication point and works with the HACA server to authenticate STAs. User authorization information is configured on the HACA server. After a user passes authentication, the HACA server authorizes network access rights to the user. **Figure 1-24** shows the HACA authentication, authorization, and accounting process.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 1-24** HACA authentication, authorization, and accounting process




1. An access device sets up a persistent connection and register with the HACA server using HTTP/2.
2. The client and device set up a pre-connection before authentication.
3. The client initiates an authentication request using HTTP. The HACA server provides a web page for the client to enter the user name and password for authentication.
4. The device and HACA server exchange authentication packets.
5. After the client passes authentication, the HACA server sends an authorization packet to authorize network access rights to the client.

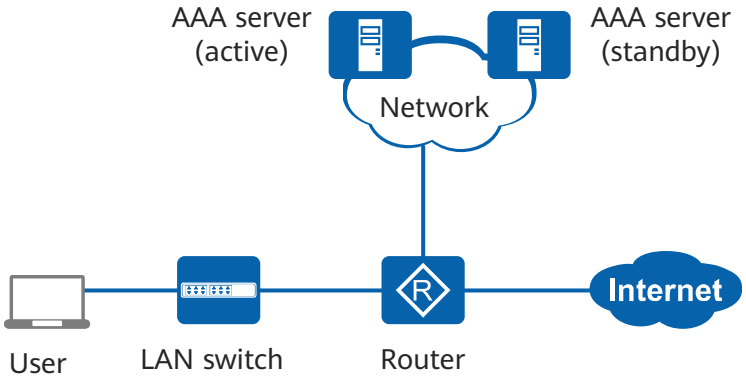
 Copyright © Huawei Technologies Co., Ltd. 

6. When the client starts to access network resources, the access device sends an accounting-start request packet to the HACA server.
7. The HACA server sends an accounting response packet to the access device and starts accounting.
8. (Optional) If real-time accounting is enabled, the access device periodically sends real-time accounting request packets to the HACA server, preventing incorrect accounting results caused by unexpected user disconnection.
9. (Optional) The HACA server returns real-time accounting response packets and performs real-time accounting.
10. The client sends a logout request.
11. The HACA server sends a logout request packet to the access device.
12. The access device sends a logout response packet to the HACA server.
13. The access device sends an accounting-stop request packet to the HACA server.
14. The HACA server sends an accounting-stop response packet to the access device and stops accounting.

# 1.3 Application Scenarios for AAA

## Deploying AAA for Internet Access Users

**Figure 1-25** AAA deployment for Internet access users




As shown in **Figure 1-25**, an enterprise network connects to the Router through the LAN switch. Users on the enterprise network need to connect to the Internet. To ensure network security, the administrator controls the Internet access rights of the users.

The administrator configures AAA on the Router to allow the Router to communicate with the AAA server. The AAA server then can manage users centrally. After a user enters the user name and password on the client, the Router forwards the authentication information including user name and password to the AAA server, and the AAA server authenticates the user. After being successfully authenticated, the user can access the Internet. The AAA server also records the network resource usage of the user.

 Copyright © Huawei Technologies Co., Ltd. 

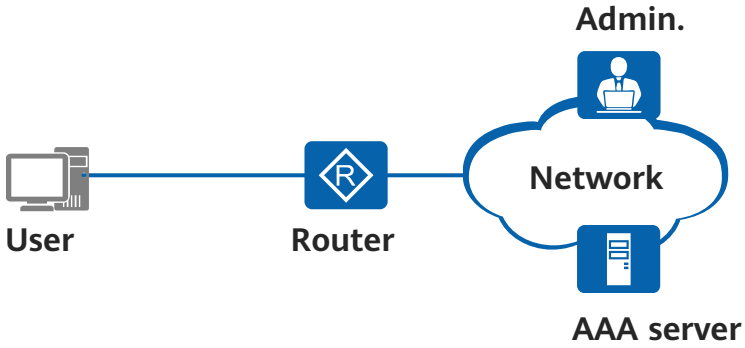
To improve reliability, two AAA servers can be deployed in active/standby mode. If the active server fails, the standby server takes over the AAA services, ensuring uninterrupted services.

## Deploying AAA for Management Users

As shown in **Figure 1-26**, the management user (Administrator) connects to the Router to manage, configure, and maintain the Router.

After the management user logs in to the Router with AAA configured, the Router sends the user name and password of the user to the AAA server. The AAA server then authenticates the user and records the user operations.

**Figure 1-26** AAA deployment for management users




## Deploying AAA for VPN Users

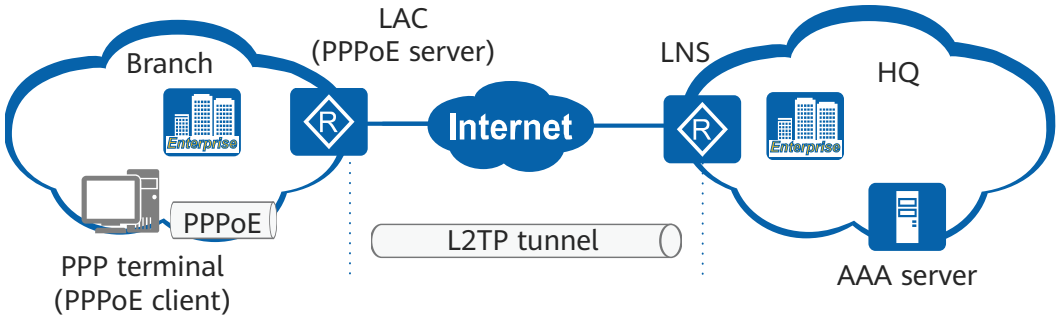
AAA is also applicable to VPN users, for example, PPP dial-up users in an L2TP VPN.

As shown in **Figure 1-27**, the headquarters (HQ) and a branch of an enterprise are located in two cities, and the branch uses an Ethernet network. Users in the branch need to access the HQ through VPDN connections. L2TP is deployed between the branch and the HQ. The branch gateway functions as a PPPoE server to allow PPP dial-up data to be transmitted over the Ethernet. The branch gateway also functions as an L2TP access concentrator (LAC) to establish L2TP tunnels with the HQ gateway that serves as the L2TP network server (LNS).

To manage access users, the LNS must have AAA authentication configured to communicate with the AAA server. The LNS sends authentication information received from dial-up users to the AAA server, and the AAA server centrally processes the information.

 Copyright © Huawei Technologies Co., Ltd. 

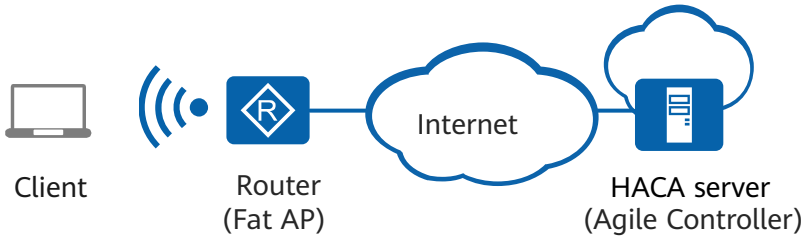
**Figure 1-27** AAA deployment for VPN users




## Deploying HACA to Authorize Users

HACA is applicable only to MAC address-prioritized portal authentication. In Figure 1-28, the router acts as a FAT AP and allows users to access the network through Wi-Fi. The Agile Controller server deployed on the cloud acts as an external portal server and HACA server to perform authentication and accounting. The router sets up a persistent connection and registers with the HACA server using HTTP/2. During portal authentication, the router and HACA server exchange packets through HTTP/2.

**Figure 1-28** Deploying HACA to Authorize Users




# 1.4 Licensing Requirements and Limitations for AAA

## Involved Network Elements

**Table 1-30** Components involved in AAA networking

| Role | Product Model | Description |
| --- | --- | --- |
| AAA server | Huawei servers or third-party AAA servers | Performs authentication, accounting, and authorization on users. |


Copyright © Huawei Technologies Co., Ltd.

### Licensing Requirements

AAA is a basic feature of a device and is not under License control.

### Feature Limitations

- To prevent data transmission risks between the device and the RADIUS or HWTACACS server, you are advised to deploy the device and RADIUS or HWTACACS server in a security domain.
- If non-authentication is configured using the **authentication-mode** command, users can pass the authentication using any user name or password. To protect the device and improve network security, you are advised to enable authentication to allow only authenticated users to access the device or network.
- By default, the accounting scheme **default** is bound to the global default common domain **default** and global default management domain **default_admin**. Modifying the accounting scheme **default** affects configurations of the two domains. Exercise caution when modifying the accounting scheme to prevent user accounting failures.
- RADIUS authentication does not take effect for L2TP access users.
- The management interface of the device cannot send or receive RADIUS packets.

## 1.5 Default Settings for AAA

**Table 1-31** describes the default settings for AAA.

**Table 1-31** Default settings for AAA

| Parameter | Default Setting |
| --- | --- |
| Local user | • Name: admin<br>• Password: The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.<br>• Access mode: SSH or HTTP (logging in to the device through the web system) |
| Global common default domain | default: By default, the authentication scheme **radius** and accounting scheme **default** are bound, and no authorization scheme is bound. |

 Copyright © Huawei Technologies Co., Ltd. 

| Parameter | Default Setting |
| --- | --- |
| Global default management domain | default_admin: By default, the authentication scheme **default** and accounting scheme **default** are bound, and no authorization scheme is bound. |
| Authentication scheme | default: Local authentication is used by default.<br>radius: RADIUS authentication is used by default. |
| Authorization scheme | default: Local authorization is used by default. |
| Accounting scheme | default: Non-accounting is used by default. |

# 1.6 Summary of AAA Configuration Tasks

In theory, the device supports the combination of authentication, authorization, and accounting. For example, the device can provide local authentication, local authorization, and RADIUS accounting.

In practice, the schemes in **Table 1-32** are often used separately. Multiple authentication or authorization modes can be used in a scheme. For example, local authentication is used as a backup of RADIUS authentication and HWTACACS authentication, and local authorization is used as a backup of HWTACACS authorization.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 1-32** AAA configuration tasks

| Configuration Task | Overview | Task |
| --- | --- | --- |
| Local authentication and authorization | If users need to be authenticated or authorized but no RADIUS server or HWTACACS server is deployed on the network, use local authentication and authorization. Local authentication and authorization feature fast processing and low operation costs; however, the amount of local authentication and authorization information that can be stored is subject to the device hardware capacity.<br>Local authentication and authorization are often used for administrators. | **1.7.1 Configuring Local Authentication and Authorization** |
| RADIUS authentication, authorization, and accounting | RADIUS protects a network from unauthorized access, and is often used on networks demanding high security and control of remote user access. | **1.7.2 Using RADIUS to Perform Authentication, Authorization, and Accounting** |
| HWTACACS authentication, authorization, and accounting | HWTACACS protects a network from unauthorized access and supports command-line authorization. HWTACACS is more reliable in transmission and encryption than RADIUS, and is more suitable for security control. | **1.7.3 Using HWTACACS to Perform Authentication, Authorization, and Accounting** |
| HACA authentication, authorization, and accounting | HACA is usually used in cloud management scenarios. HACA is based on HTTP/2 and only supports MAC address-prioritized authentication. | **1.7.4 Configuring HACA Authentication** |

# 1.7 Configuring AAA

## 1.7.1 Configuring Local Authentication and Authorization


Copyright © Huawei Technologies Co., Ltd.

## Local Authentication and Authorization

After local authentication and authorization are configured, the device authenticates and authorizes access users based on local user information. In local authentication and authorization, user information, including the local user name, password, and attributes, is configured on the device. Local authentication and authorization feature fast processing and low operation cost. However, the amount of local authentication and authorization information that can be stored is subject to the device hardware capacity.

## Configuration Procedure

| Configuration | Procedure | Description |
| --- | --- | --- |
| Configure a local server. | Configure a local user. | Create a local user. The device authenticates the local user using the created user information. |
| | Configure local authorization rules. | Create authorization rules. The device authorizes the user based on the created authorization rules. |
| Configure and apply AAA schemes. | Configure AAA schemes. | Configure authentication, authorization, and accounting schemes. |
| | (Optional) Configure a service scheme. | User authorization information can also be configured in the service scheme. |
| | Apply the AAA schemes to a domain. | The created AAA schemes and service scheme take effect only after they are applied to the domain to which users belong. |
| - | Verify the configuration. | Verify the configuration. |

## 1.7.1.1 Configuring a Local Server

## Context

AAA authentication and authorization can be implemented on a network access server (NAS) device or a server. If AAA authentication and authorization are implemented on the NAS, a local AAA server is configured on the NAS. Local authentication features fast processing and low operation costs. However, how much user information can be stored depends on the hardware capacity of the device.

To configure a local server, you need to configure user authentication and authorization information on the device, including configuring a local user and configuring local authorization.

 Copyright © Huawei Technologies Co., Ltd. 

### 1.7.1.1.1 Configuring a Local User

## Context

When configuring a local user, you can configure the number of connections that can be established by the local user, local user level, idle timeout period, and login time, and allow the local user to change the password.

NOTE

- To ensure device security, enable password complexity check and change the password periodically.
- After you change the local account's rights (including the password, access type, FTP directory, and level), the rights of users who are already online remain unchanged. Rather, the rights are only changed once a user goes online again.
- Local users' access types include:
  - Administrative: **ftp**, **http**, **ssh**, **telnet**, **x25-pad**, and **terminal**
  - Common: **802.1x**, **bind**, **ppp**, **sslvpn**, and **web**
- Security risks exist if the user login mode is set to Telnet or FTP. You are advised set the user login mode to STelnet or SFTP and set the user access type to SSH.

  When a device starts without any configuration, HTTP uses the randomly generated self-signed certificate to support HTTPs. The self-signed certificate may bring risks. Therefore, you are advised to replace it with the officially authorized digital certificate.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **aaa**

The AAA view is displayed.

**Step 3** Create a local user.

| Procedure | Command | Description |
| --- | --- | --- |
| (Optional) Enable the password complexity check. | **user-password complexity-check** | By default, the password complexity check is enabled. |
| Create a local user name and a password (using either of the | **local-user** *user-name* **password** | The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the |

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | Command | Description |
| --- | --- | --- |
| commands). | **local-user** *user-name* **password** { **cipher** \| **irreversible-cipher** } *password* | website to find out how to obtain it.<br>This command should be entered in interactive mode. This is because directly entering a plain text password without being in interactive mode poses potential security risks.<br>If a user name contains a domain name delimiter (such as @, \|, or %) and the domain name parsing direction is not configured using the **domainname-parse-direction right-to-left** command, the character string before the delimiter is considered as the user name, and that after the delimiter is considered as the domain name. If a user name does not contain a domain name delimiter, the entire character string is considered as the user name. By default, common users are authenticated in the domain **default**, and administrators are authenticated in the domain **default_admin**. |
| Configure an access type for the local user. | **local-user** *user-name* **service-type** { **8021x** \| **bind** \| **ftp** \| **http** \| **ppp** \| **ssh** \| **sslvpn** \| **telnet** \| **terminal** \| **web** \| **x25-pad** } * | By default, all access types are disabled for a local user.<br>The access type configured for portal access users is **web**.<br>If the user exists, note that:<br>• If the irreversible password algorithm is used, the access type can only be administrative.<br>• If the reversible password algorithm is used, the access type can be common or administrative, but cannot be a combination of common and administrative. In addition, when the access type is set to an administrative type, the password encryption algorithm is automatically changed to the irreversible algorithm. |

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | Command | Description |
| --- | --- | --- |
| (Optional) Allocate a fixed IP address to the local user. | **local-user** *user-name* **bind-ip** *ip-address* | By default, no fixed IP address is allocated to the local user. |

**Step 4** (Optional) Set the user level, user group, access time range, idle timeout period, and number of connections that can be established by the user.

| Procedure | Command | Description |
| --- | --- | --- |
| Set the local user level. | **local-user** *user-name* **privilege level** *level* | The default level of a local user is 0. |
| Set the local user group. | **local- user** *user-name* **user-group** *group-name* | By default, a local user does not belong to any group. |
| Set the access time range for the local user. | **local-user** *user-name* **time-range** *time-name* | By default, no access time range is configured and the local user can access the network anytime. |
| Set the idle timeout period for the specified user. | **local-user** *user-name* **idle-timeout** *minutes* [ *seconds* ] or **local-user** *user-name* **idle-cut** | You can specify the idle timeout period. If the local user is idle for longer than the specified period, the user automatically goes offline.<br>If the idle timeout period is set to 0 or a large value, the terminal will remain in the login state, resulting in security risks. Instead, you are advised to run the **lock** command to lock the connection.<br>To enable idle-cut for common users (NAC or PPP users), run the **local-user** *user-name* **idle-cut** command. To enable idle-cut for administrators, run the **local-user** *user-name* **idle-timeout** *minutes* [ *seconds* ] command. |

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | Command | Description |
| --- | --- | --- |
| Set the maximum number of connections that can be established by the local user. | **local-user** *user-name* **access-limit** *max-number* | By default, the number of connections that can be established by a user is not limited.<br>To configure the local account to be logged in to on only one terminal, set *max-number* to 1. |

**Step 5** (Optional) Configure security of the local user.

| Procedure | Command | Description |
| --- | --- | --- |
| Enable the local account lock function, and set the retry interval, maximum number of consecutive authentication failures, and account lock period. | **local-aaa-user wrong-password retry-interval** *retry-interval* **retry-time** *retry-time* **block-time** *block-time* | By default, the local account lock function is enabled, the retry interval is 5 minutes, the maximum number of consecutive authentication failures is 3, and the account lock period is 5 minutes. |
| Configure the user to access the network using specified IP addresses when the user account is locked. | **aaa-quiet administrator except-list** { *ipv4-address* \| *ipv6-address* } &<1-32> | By default, a user cannot access the network when the account is locked.<br>To check information about the specified IP addresses, run the **display aaa-quiet administrator except-list** command. |

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | | Command | Description |
| --- | --- | --- | --- |
| Configure the password policy for local access users. | Enable the password policy for local access users and enter the local access user password policy view. | **local-aaa-user password policy access-user** | By default, the password policy for local access users is disabled. |
| | Set the maximum number of historical passwords recorded for each user. | **password history record number** *number* | By default, a maximum of five historical passwords are recorded for each user. |
| | Exit the local access user password policy view. | **quit** | - |

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | | Command | Description |
| --- | --- | --- | --- |
| Configure the password policy for local administrators. | Enable the password policy for local administrators and enter the local administrator password policy view. | **local-aaa-user password policy administrator** | By default, the password policy of local administrators is disabled. |
| | Enable the password expiration prompt function and set the password expiration prompt period. | **password alert before-expire** *day* | By default, the system displays a prompt 30 days before the password expires. |
| | Enable the initial password change prompt function. | **password alert original** | By default, the system prompts users to change initial passwords. |

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | | Command | Description |
| --- | --- | --- | --- |
| | Enable the password expiration function and set the password validity period. | **password expire** *day* | By default, the password validity period is 90 days. |
| | Set the maximum number of historical passwords recorded for each user. | **password history record number** *number* | By default, a maximum of five historical passwords are recorded for each user. |
| | Exit the local administrator password policy view. | **quit** | - |

**Step 6** (Optional) Set parameters of access rights for the local user.

| Procedure | Command | Description |
| --- | --- | --- |
| Configure the FTP directory that FTP users can access. | **local-user** *user-name* **ftp-directory** *directory* | By default, the FTP directory that FTP users can access is not configured.<br>If the access type of the local user is FTP, you must configure the FTP directory, and set the local user level to be lower than the management level; otherwise, the FTP user cannot log in to the device. |

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | Command | Description |
| --- | --- | --- |
| Set the local user state. | **local-user** *user-name* **state** { **active** \| **block** } | By default, a local user is in the active state.<br>The device processes requests from users in different states as follows:<br>• If the local user is in the active state, the device accepts and processes the authentication request from the user.<br>• If the local user is in the block state, the device rejects the authentication request from the user. |
| Set the expiration date for the local account. | **local-user** *user-name* **expire-date** *expire-date* | By default, a local account is permanently valid. |
| Set the account type of the local user. | **local-user** *user-name* **account-type cmcc-tr069** | By default, the account type of a local user is not specified.<br>If the TR-069 function is not enabled by the **set operator-code cmcc** command, this command cannot be executed. |

**Step 7** (Optional) Change the login password of the local user.

| Procedure | Command | Description |
| --- | --- | --- |
| Return to the user view. | **return** | - |
| Change the login password of the local user. | **local-user change-password** | - |

**----End**

### 1.7.1.1.2 Configuring Authorization Rules

## Context

Table 1-33 describes authorization parameters that can be set locally during local authorization configuration.

**Table 1-33** Local authorization parameters

| Authorization Parameter | Usage Scenario | Description |
| --- | --- | --- |
| VLAN | VLAN-based authorization is easy to deploy and maintenance costs are low. It applies to scenarios where employees in an office or a department have the same access rights. | In local authorization, you only need to configure VLANs and corresponding network resources on the device.<br>An authorized VLAN cannot be delivered to online Portal users.<br>After a user is authorized based on a VLAN, the user needs to manually trigger an IP address request using DHCP. |
| Service scheme | A service scheme and corresponding network resources need to be configured on the device. | You need to configure a service scheme and corresponding network resources on the device.<br>A service scheme can be applied to a domain, and users in the domain then can obtain authorization information in the service scheme. |
| User group | A user group consists of users (terminals) with the same attributes, such as the role and rights. For example, according to the enterprise department structure, you can divide users on a campus network into different groups, such as R&D group, finance group, marketing group, and guest group, and perform different security policies for these groups. | In local authorization, all you need to do is configure user groups and corresponding network resources on the device.<br>A user group can be applied to a domain, and users in the domain then can obtain authorization information in the user group.<br>For details on how to configure a user group, see **Configure an authorization user group**. |

## Procedure

- Configure an authorization VLAN.

  Configure a VLAN and the network resources in the VLAN on the device.

 Copyright © Huawei Technologies Co., Ltd. 

- Configure a service scheme.

  For details on how to configure a service scheme, see **1.7.1.3 (Optional) Configuring a Service Scheme**.
- Configure an authorization user group.

  For details about how to configure an authorized user group, see the table below.

| Procedure | Command | Description |
| --- | --- | --- |
| Create a user group and enter the user group view. | **user-group** *group-name* | When using a user group in a hot standby scenario or a dual-link backup scenario, specify the user group index, and ensure that the user group name and index specified on the active device are the same as those specified on the standby device. |
| Bind an ACL to the user group. | **acl-id** *acl-number* | By default, no ACL is bound to a user group.<br>The IPv4 ACL to be bound to a user group must have been created using the **acl (system view)** command. |
| Set the priority for the user group. | **remark** { **8021p** *8021p-value* \| **dscp** *dscp-value* \| **exp** *exp-value* \| **lp** *lp-value* }* | By default, the user group priority is not specified. |

**----End**

## 1.7.1.2 Configuring AAA Schemes

## Context

To use local authentication and authorization, set the authentication mode in an authentication scheme to local authentication and the authorization mode in an authorization scheme to local authorization.

By default, the device performs local authentication and authorization for access users.

NOTE

If non-authentication is configured using the **authentication-mode** command, users can pass the authentication using any user name or password. To protect the device and improve network security, you are advised to enable authentication to allow only authenticated users to access the device or network.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

- Configure an authentication scheme.
  a. Run **system-view**

     The system view is displayed.
  b. Run **aaa**

     The AAA view is displayed.
  c. Run **authentication-scheme** *authentication-scheme-name*

     An authentication scheme is created and the authentication scheme view is displayed, or an existing authentication scheme view is displayed.

     Two default authentication schemes named **default** and **radius** are available on the device. These two authentication schemes can be modified but not deleted.
  d. Run **authentication-mode local**

     The authentication mode is set to local.

     By default, local authentication is used.
  e. (Optional) Run **authentication-super** [ **hwtacacs** | **super** ] * **none**

     An authentication mode for upgrading user levels is set.

     The default mode is **super** (local authentication).
  f. Run **quit**

     The AAA view is displayed.
  g. (Optional) Run **domainname-parse-direction** { **left-to-right** | **right-to-left** }

     The direction in which the domain name is parsed is specified.

     By default, a domain name is parsed from left to right.
  h. Run **quit**

     The system view is displayed.
  i. (Optional) Run **aaa-authen-bypass enable time** *time-value*

     The bypass authentication duration is set.

     By default, the bypass authentication function is disabled.
- Configure an authorization scheme.
  a. Run **system-view**

     The system view is displayed.
  b. Run **aaa**

     The AAA view is displayed.
  c. Run **authorization-scheme** *authorization-scheme-name*

     An authorization scheme is created and the authorization scheme view is displayed, or an existing authorization scheme view is displayed.

 Copyright © Huawei Technologies Co., Ltd. 

A default authorization scheme named **default** is available on the device. This authorization scheme can be modified but not deleted.

d. Run **authorization-mode local** [ **none** ]

The authorization mode is set.

By default, local authorization is used.

e. Run **quit**

The AAA view is displayed.

f. (Optional) Run **authorization-modify mode** { **modify** | **overlay** }

The update mode of user authorization information delivered by the authorization server is set.

The default mode is **overlay**.

g. Run **quit**

The system view is displayed.

h. (Optional) Run **aaa-author-bypass enable time** *time-value*

The bypass authorization duration is set.

By default, the bypass authorization function is disabled.

**----End**

### 1.7.1.3 (Optional) Configuring a Service Scheme

#### Context

Users must obtain authorization information before going online. You can configure a service scheme to manage authorization information about users.

#### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **aaa**

The AAA view is displayed.

**Step 3** Run **service-scheme** *service-scheme-name*

A service scheme is created and the service scheme view is displayed.

By default, no service scheme is configured on the device.

**Step 4** Run **admin-user privilege level** *level*

The user is configured as the administrator and the administrator level for login is specified.

The value range of *level* is from 0 to 15. By default, the user level is not specified.

**Step 5** Configure server information.

 Copyright © Huawei Technologies Co., Ltd. 

| Step | Command | Remarks |
| --- | --- | --- |
| Configure a DHCP server group. | **dhcp-server group** *group-name* | By default, no DHCP server group is configured in a service scheme. |
| Configure the IP address of the primary DNS server. | **dns** *ip-address* | By default, no primary DNS server is configured in a service scheme. |
| Configure the IP address of the secondary DNS server. | **dns** *ip-address* **secondary** | By default, no secondary DNS server is configured in a service scheme. |

**Step 6** Configure resources delivered by the server in an Efficient VPN scenario.

| Step | Command | Remarks |
| --- | --- | --- |
| Configure the primary WINS server. | **wins** *ip-address* | By default, no primary WINS server is configured in a service scheme. |
| Configure the secondary WINS server. | **wins** *ip-address* **secondary** | By default, no secondary WINS server is configured in a service scheme. |
| Configure the URL and version number in the service scheme. | **auto-update url** *url-string* **version** *version-number* | By default, no URL or version number is configured in a service scheme. |

 Copyright © Huawei Technologies Co., Ltd. 

| Step | Command | Remarks |
| --- | --- | --- |
| Configure the default DNS domain name in the service scheme. | **dns-name** *domain-name* | By default, no default DNS domain name is configured in a service scheme. |
| Configure the local subnet information to be sent to the remote end. | **route set acl** *acl-number* | By default, no local subnet information is sent to the remote end. |
| Configure the IP address of the interface bound to the IPSec tunnel to be sent to the remote end. | **route set interface** | By default, no IP address of the interface bound to the IPSec tunnel is sent to the remote end. |

**Step 7** Run **ip-pool** *pool-name* [ **move-to** *new-position* ]

An IP address pool is bound to the service scheme or an existing IP address pool is moved.

By default, no IP address pool is bound to a service scheme.

NOTE

Ensure that the IP address pool has been configured before running this command.

**Step 8** Run **qos-profile** *profile-name*

A QoS profile is bound to the service scheme.

By default, no QoS profile is bound to a service scheme.

NOTE

Ensure that the QoS profile has been configured before running this command.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 9** Run **idle-cut** *idle-time flow-value* [ **inbound** | **outbound** ]

The idle-cut function is enabled for domain users and the idle-cut parameters are set.

By default, the idle-cut function is disabled for domain users.

NOTE

The idle-cut function takes effect only after the idle time and traffic threshold are configured. To configure the traffic threshold, run the **idle-cut** *idle-time flow-value* command. To configure the idle time, use the value of *idle-time* configured on the device or the value (carried in RADIUS attribute 28 Idle-Timeout) authorized by the RADIUS server. If both values exist, the value authorized by the RADIUS server has a higher priority.

The **idle-cut** command configured in the service scheme view takes effect for administrators. For common users, the function takes effect only for PPPoE and Portal users.

**----End**

## 1.7.1.4 Applying AAA Schemes to a Domain

## Context

The created authentication and authorization schemes take effect only after being applied to a domain. When local authentication and authorization are used, the default accounting scheme non-accounting is used.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **aaa**

The AAA view is displayed.

**Step 3** Run **domain** *domain-name* [ **domain-index** *domain-index* ]

A domain is created and the domain view is displayed, or the view of an existing domain is displayed.

The device has two default domains:

- **default**: Used by common access users
- **default_admin**: Used by administrators

NOTE

- If a user enters a user name that does not contain a domain name, the user is authenticated in the default domain. In this case, you need to run the **domain** *domain-name* [ **admin** ] command and set *domain-name* to configure a global default domain on the device.
- If a user enters a user name that contains a domain name during authentication, the user must enter the correct value of *domain-name*.

**Step 4** Apply AAA schemes to the domain.

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | Command | Description |
| --- | --- | --- |
| Apply an authentication scheme to the domain. | **authentication-scheme** *authentication-scheme-name* | By default, the authentication scheme named **radius** is applied to the **default** domain, the authentication scheme named **default** is applied to the **default_admin** domain, and the authentication scheme named **default** is applied to other domains. |
| Apply an authorization scheme to the domain. | **authorization-scheme** *authorization-scheme-name* | By default, no authorization scheme is applied to a domain. |

**Step 5** Configure local authorization rules.

| Procedure | Command | Description |
| --- | --- | --- |
| (Optional) Apply a user group to the domain. | **user-group** *group-name* | By default, no user group is applied to a domain. |
| (Optional) Apply a service scheme to the domain. | **service-scheme** *service-scheme-name* | By default, no service scheme is applied to a domain. |

**Step 6** (Optional) Specify the domain state and enable traffic statistics collection for the domain.

| Procedure | Command | Description |
| --- | --- | --- |
| Specify the domain state. | **state** { **active** \| **block** [ **time-range** *time-name* &<1–4> ] } | When a domain is in the blocking state, users in this domain cannot log in. By default, a created domain is in the active state. |

**Step 7** (Optional) Run **statistic enable**

Traffic statistics collection is enabled for users in the domain.

By default, traffic statistics collection is disabled for users in a domain.

**Step 8** (Optional) Configure a domain name parsing scheme. (If domain name parsing is configured in both the AAA view and authentication profile view, the device preferentially uses the configuration in the authentication profile. The configuration in the authentication profile applies only to wireless users.)

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | | Command | Description |
| --- | --- | --- | --- |
| AAA view | Exit from the domain view. | **quit** | - |
| | Specify the domain name parsing direction. | **domainname-parse-direction** { **left-to-right** \| **right-to-left** } | The domain name can be parsed from left to right, or from right to left.<br>By default, the domain name is parsed from left to right. |
| | Set the domain name delimiter. | **domain-name-delimiter** *delimiter* | A domain name delimiter can be any of the following: \ / : < > \| @ ' %.<br>The default domain name delimiter is @. |
| | Specify the domain name location. | **domain-location** { **after-delimiter** \| **before-delimiter** } | The domain name can be placed before or after the delimiter.<br>By default, the domain name is placed after the domain name delimiter. |
| | Set the security string delimiter. | **security-name-delimiter** *delimiter* | The default security string delimiter is * (asterisk). |

**----End**

## 1.7.1.5 Verifying the Local Authentication and Authorization Configuration

## Procedure

- Run the **display aaa configuration** command to check the AAA summary.
- Run the **display authentication-scheme** [ *authentication-scheme-name* ] command to verify the authentication scheme configuration.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **display authorization-scheme** [ *authorization-scheme-name* ] command to verify the authorization scheme configuration.
- Run the **display access-user** [ **domain** *domain-name* | **interface** *interface-type interface-number* [ **vlan** *vlan-id* [ **qinq** *qinq-vlan-id* ] ] | **ip-address** *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **ipv6-address** *ipv6-address* | **access-slot** *slot-id* | **user-group** *user-group-name* | **username** *user-name* ] [ **detail** ], **display access-user** [ **mac-address** *mac-address* | **service-scheme** *service-scheme-name* | **user-id** *user-id* | **statistics** | **ssid** *ssid-name* ], or **display access-user access-type** { **admin** [ **ftp** | **ssh** | **telnet** | **terminal** | **web** ] | **ppp** | **l2tp** } [ **username** *user-name* ] command to check the summary of online users.
- Run the **display domain** [ **name** *domain-name* ] command to verify the domain configuration.
- Run the **display local-user** [ **domain** *domain-name* | **state** { **active** | **block** } | **username** *username* ] * command to check the brief information about local users.
- Run the **display local-user expire-time** command to verify the time when the local account expires.
- Run the **display aaa statistics access-type-authenreq** command to verify the number of authentication requests.

**----End**

# 1.7.2 Using RADIUS to Perform Authentication, Authorization, and Accounting

## RADIUS Authentication, Authorization, and Accounting

Remote Authentication Dial-In User Service (RADIUS) is often used to implement authentication, authorization, and accounting (AAA). It uses the client/server model and prevents unauthorized access to networks that require high security and control of remote user access.

## Configuration Procedure

## 1.7.2.1 Configuring an AAA Scheme

## Context

An AAA scheme defines the authentication, authorization, and accounting modes used by users. If RADIUS AAA is used, set the authentication mode to RADIUS in the authentication scheme, and set the accounting mode to RADIUS in the accounting scheme. RADIUS authentication is combined with authorization and cannot be separated. If authentication succeeds, authorization also succeeds. If RADIUS authentication is used, you do not need to configure an authorization scheme.

To prevent authentication failures caused by no response from a single authentication mode, configure local authentication or non-authentication as the backup authentication mode in the authentication scheme.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

If non-authentication is configured using the **authentication-mode** command, users can pass the authentication using any user name or password. To protect the device and improve network security, you are advised to enable authentication to allow only authenticated users to access the device or network.

## Procedure

- Configure an authentication scheme.
  a. Run **system-view**

     The system view is displayed.
  b. Run **aaa**

     The AAA view is displayed.
  c. Run **authentication-scheme** *scheme-name*

     An authentication scheme is created and the authentication scheme view is displayed, or the view of an existing authentication scheme is displayed.

     By default, two authentication schemes named **default** and **radius** are available on the device. The two schemes can only be modified, but cannot be deleted.
  d. Run **authentication-mode radius**

     The authentication mode is set to RADIUS.

     By default, local authentication is used.

     To configure local authentication as the backup authentication mode, run the **authentication-mode radius local** command.
  e. Run **quit**

     Return to the AAA view.
  f. (Optional) Configure the account locking function.
     i. Run **remote-aaa-user authen-fail retry-interval** *retry-interval* **retry-time** *retry-time* **block-time** *block-time*

        The remote AAA authentication account locking function is enabled, and the authentication retry interval, maximum number of consecutive authentication failures, and account locking period are configured.

        By default, the remote AAA account locking function is enabled, the authentication retry interval is 300 minutes, the maximum number of consecutive authentication failures is 30, and the account locking period is 30 minutes.
     ii. Run **aaa-quiet administrator except-list** { *ipv4-address* | *ipv6-address* } &<1-32>

        A user is configured to access the network using a specified IP address if the user account is locked.

        By default, a user cannot access the network if the user account is locked.

 Copyright © Huawei Technologies Co., Ltd. 

You can run the **display aaa-quiet administrator except-list** command to query the specified IP addresses.

iii. Run **remote-user authen-fail unblock** { **all** | **username** *username* }

A remote AAA authentication account that has failed authentication is unlocked.

g. (Optional) Run **aaa-author session-timeout invalid-value enable**

The device is disabled from disconnecting or reauthenticating users when the RADIUS server delivers the Session-Timeout attribute with value 0.

By default, when the RADIUS server delivers the Session-Timeout attribute with value 0, this attribute does not take effect.

h. Run **quit**

Return to the system view.

i. (Optional) Run **aaa-authen-bypass enable time** *time-value*

The bypass authentication timeout interval is configured.

By default, the bypass authentication function is disabled.

- Configure an accounting scheme.
  a. Run **system-view**

  The system view is displayed.

  b. Run **aaa**

  The AAA view is displayed.

  c. Run **accounting-scheme** *accounting-scheme-name*

  An accounting scheme is created and the accounting scheme view is displayed, or the view of an existing accounting scheme is displayed.

  By default, the accounting scheme named **default** is available on the device. This scheme can only be modified, but cannot be deleted.

  d. Run **accounting-mode radius**

  The accounting mode is set to RADIUS.

  By default, the accounting mode is **none**.

  e. (Optional) Configure policies for accounting failures.

  - Configure a policy for accounting-start failures.

    Run **accounting start-fail** { **offline** | **online** }

    A policy for accounting-start failures is configured.

    By default, users cannot go online if accounting-start fails.

  - Configure a policy for real-time accounting failures.

    1) Run **accounting realtime** *interval*

    The real-time accounting function is enabled, and the interval for real-time accounting is configured.

    By default, the device performs accounting based on the user online duration, and the real-time accounting function is disabled.

 Copyright © Huawei Technologies Co., Ltd. 

2) Run **accounting interim-fail** [ **max-times** *times* ] { **offline** | **online** }

The maximum number of real-time accounting failures and a policy used after the number of real-time accounting failures exceeds the maximum are configured.

By default, the maximum number of real-time accounting failures is 3, and the device keeps users online after the number of real-time accounting failures exceeds the maximum.

- Configure a policy for accounting-stop failures.

1) Run **quit**

Return to the AAA view.

2) Run **quit**

Return to the system view.

3) Run **radius-server template** *template-name*

The RADIUS server template view is displayed.

4) Run **radius-server accounting-stop-packet resend** [ *resend-times* ]

Retransmission of accounting-stop packets is enabled, and the number of accounting-stop packets that can be retransmitted each time is configured.

By default, retransmission of accounting-stop packets is enabled, and the retransmission times is 3.

f. (Optional) Run **quit**

Return to the system view.

g. (Optional) Run **authentication-profile name** *authentication-profile-name*

The authentication profile view is displayed.

By default, the device has six built-in authentication profiles: default_authen_profile, dot1x_authen_profile, mac_authen_profile, portal_authen_profile, dot1xmac_authen_profile, and multi_authen_profile.

h. (Optional) Run **authentication { roam-accounting | update-ip-accounting }** * **enable**

The device is configured to send accounting packets upon roaming and address updating.

By default, the device sends accounting packets upon roaming and address updating.

After the roaming accounting function is enabled for multi-link accounting users, you need to run the **authentication roam-accounting update-session-mode** command to enable the accounting session update mode during roaming accounting.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## Verifying the Configuration

- Run the **display authentication-scheme** [ *authentication-scheme-name* ] command to view the authentication scheme configuration.
- Run the **display accounting-scheme** [ *accounting-scheme-name* ] command to view the accounting scheme configuration.

## 1.7.2.2 Configuring a RADIUS Server Template

## Context

You can specify the RADIUS server connected to the device in a RADIUS server template. Such a template contains the server IP address, port number, source interface, and shared key settings.

The settings in a RADIUS server template must be the same as those on the RADIUS server.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **radius-server template** *template-name*

The RADIUS server template view is displayed.

By default, the RADIUS server template named **default** is available on the device. This template can only be modified, but cannot be deleted.

**Step 3** Configure RADIUS authentication and accounting servers.

| Step | Command | Remarks |
| --- | --- | --- |
| Configure a RADIUS authentication server. | • IPv4 server: **radius-server authentication** *ipv4-address port* [ **vpn-instance** *vpn-instance-name* \| **source** { **loopback** *interface-number* \| **ip-address** *ipv4-address* \| **vlanif** *interface-number* } \| **weight** *weight-value* ] *<br>• IPv6 server: **radius-server authentication** *ipv6-address port* [ **source** { **loopback** *interface-number* \| **ip-address** *ipv6-address* \| **vlanif** *interface-number* } \| **weight** *weight-value* ] * | By default, no RADIUS authentication server is configured. |

 Copyright © Huawei Technologies Co., Ltd. 

| Step | Command | Remarks |
| --- | --- | --- |
| Configure a RADIUS accounting server. | • IPv4 server: **radius-server accounting** *ipv4-address port* [ **vpn-instance** *vpn-instance-name* \| **source** { **loopback** *interface-number* \| **ip-address** *ipv4-address* \| **vlanif** *interface-number* } \| **weight** *weight-value* ] *<br>• IPv6 server: **radius-server accounting** *ipv6-address port* [ **source** { **loopback** *interface-number* \| **ip-address** *ipv6-address* \| **vlanif** *interface-number* } \| **weight** *weight-value* ] * | By default, no RADIUS accounting server is configured. |

**Step 4** Run **radius-server shared-key cipher** *key-string*

The shared key of the RADIUS server is configured.

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

NOTE

When a RADIUS server is configured in multiple RADIUS server templates:

- If the RADIUS server templates use different shared keys, you need to configure the shared keys in each RADIUS server template view.
- If the RADIUS server templates use the same shared key, you can configure the shared key in the system view using the **radius-server ip-address** { *ipv4-address* | *ipv6-address* } **shared-key cipher** *key-string* command.
- When shared keys are configured in both the RADIUS server template view and system view, the configuration in the system view takes effect.

**Step 5** (Optional) Run **radius-server algorithm** { **loading-share** | **master-backup** } [ **based-user** ]

The algorithm for selecting RADIUS servers is configured.

By default, the algorithm for selecting RADIUS servers is primary/secondary (specified by **master-backup**).

When multiple authentication or accounting servers are configured in a RADIUS server template, the device selects RADIUS servers based on the configured algorithm and the weight configured for each server.

- When the algorithm for selecting RADIUS servers is set to primary/secondary, the server with a larger weight is the primary server. If servers have the same weight, the server configured first is the primary server.
- If the algorithm for selecting RADIUS servers is set to load balancing, packets are sent to RADIUS servers according to weights of the servers.

**Step 6** (Optional) Run **radius-server** { **retransmit** *retry-times* | **timeout** *time-value* } *

The number of times that RADIUS request packets are retransmitted and the timeout interval are set.

 Copyright © Huawei Technologies Co., Ltd. 

By default, RADIUS request packets can be retransmitted three times, and the timeout interval is 5 seconds.

**Step 7** (Optional) Configure the format of the user name in packets sent from the device to the RADIUS server.

- Run **radius-server user-name domain-included**

  The device is configured to encapsulate the domain name in the user name in the RADIUS packets sent to a RADIUS server.
- Run **radius-server user-name original**

  The device is configured not to modify the user name entered by a user in the RADIUS packets sent to a RADIUS server.
- Run **undo radius-server user-name domain-included**

  The device is configured not to encapsulate the domain name in the user name in the RADIUS packets sent to a RADIUS server.
- Run **undo radius-server user-name domain-included except-eap**

  The device is configured not to encapsulate the domain name in the user name in the RADIUS packets sent to a RADIUS server (applicable to other authentication modes except EAP authentication).

By default, the device does not modify the user name entered by a user in the RADIUS packets sent to a RADIUS server.

**Step 8** (Optional) Run **radius-server traffic-unit** { **byte** | **kbyte** | **mbyte** | **gbyte** }

The traffic unit used by the RADIUS server is configured.

By default, the RADIUS traffic unit is byte on the device.

**Step 9** (Optional) Run **radius-attribute service-type with-authenonly-reauthen**

The reauthentication mode is set to reauthentication only.

By default, the reauthentication mode is reauthentication and reauthorization.

This function takes effect when the Service-Type attribute on the RADIUS server is set to **Authenticate Only**.

**----End**

## Verifying the Configuration

Run the **display radius-server configuration** [ **template** *template-name* ] command to check the RADIUS server template configuration.

## Verifying the Connectivity Between the Device and RADIUS Server

Run the **test-aaa** *user-name user-password* **radius-template** *template-name* [ **chap** | **pap** | **accounting** [ **start** | **realtime** | **stop** ] ] command to check the connectivity between the device and the RADIUS authentication or accounting server. Only when they are reachable, the authentication or accounting server can perform authentication or accounting properly for users.

If an error message is displayed in the command output, troubleshoot the fault by referring to **Testing Whether a User Can Pass RADIUS Authentication or Accounting**.

 Copyright © Huawei Technologies Co., Ltd. 

### 1.7.2.3 (Optional) Configuring the RADIUS Server Status Detection Function

## Context

A device can detect the RADIUS server status using the RADIUS server status detection function. If the RADIUS server status is Down, users can obtain escape rights. If the RADIUS server status reverts to Up, escape rights are removed from the users and the users are reauthenticated.

## Procedure

- Configure conditions for setting the RADIUS server status to Down.
  - Conditions for setting the RADIUS server status to Down during the RADIUS server status detection.
    i. Run **system-view**
    The system view is displayed.
    ii. Run **radius-server** { **dead-interval** *dead-interval* | **dead-count** *dead-count* }
    The RADIUS server detection interval and maximum number of consecutive unacknowledged packets in each detection interval are configured.
    iii. Run the **return** command to return to the user view.
- (Optional) Configure the automatic detection function.
  a. Run **system-view**
  The system view is displayed.
  b. Run **radius-server template** *template-name*
  The RADIUS server template view is displayed.
  c. Run **radius-server testuser username** *user-name* **password cipher** *password*
  A user account for automatic RADIUS server detection is created.
  By default, no RADIUS template-based user account for automatic detection is configured.
  After the user account for automatic RADIUS server detection is created, the automatic detection function is enabled.
  d. (Optional) Run **radius-server detect-server interval** *interval*
  The automatic detection interval for RADIUS servers is configured.
  By default, the automatic detection interval for RADIUS servers is 60 seconds.
  e. Run the **return** command to return to the user view.
- (Optional) Configure the duration for which a RADIUS server remains Down, namely, configure the Force-up timer.

  NOTE

  After setting the RADIUS server status to Force-up and automatic detection is enabled, the device immediately sends a detection packet. If the device receives a response packet from the RADIUS server within the timeout period, the device sets the RADIUS server status to Up; otherwise, the device sets the RADIUS server status to Down.

 Copyright © Huawei Technologies Co., Ltd. 

a. Run **system-view**

The system view is displayed.

b. Run **radius-server template** *template-name*

The RADIUS server template view is displayed.

c. Run **radius-server dead-time** *dead-time*

The Force-up timer for RADIUS servers is configured.

By default, the Force-up timer for RADIUS servers is 5 minutes.

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

- (Optional) Configure status synchronization between RADIUS authentication and accounting servers.

a. Run **system-view**

The system view is displayed.

b. Run the **radius-server dead-detect-condition by-server-ip** command to configure IP address-based automatic detection for RADIUS servers.

By default, RADIUS authentication and accounting servers are detected separately. After this function is configured, RADIUS authentication and accounting servers with the same IP address in the same VPN instance are detected together and their status are updated at the same time.

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

**----End**

## Verifying the Configuration

- Run the **display radius-server** { **dead-interval** | **dead-count** } command to check configuration information about the RADIUS server detection interval and maximum number of consecutive unacknowledged packets in each detection interval.
- Run the **display radius-server configuration** command to check configuration information about the user account for automatic detection, detection interval, and timeout period for detection packets in the RADIUS server template.

## Follow-up Procedure

1. Run the **authentication event authen-server-down action authorize** command in the authentication profile view to configure the user escape function if the authentication server goes Down. For details, see **3.6.3.4 (Optional) Configuring Authentication Event Authorization Information** in **NAC Configuration**.
2. Run the **authentication event authen-server-up action re-authen** command in the authentication profile view to configure the reauthentication function after the authentication server reverts to the Up status. For details, see **3.6.3.6 (Optional) Configuring Re-authentication for Users** in **NAC Configuration**.

# 1.7.2.4 (Optional) Configuring RADIUS Attributes

 Copyright © Huawei Technologies Co., Ltd. 

### 1.7.2.4.1 Disabling or Translating RADIUS Attributes

## Context

RADIUS attributes supported by different vendors are incompatible with each other, so RADIUS attributes must be disabled or translated in interoperation and replacement scenarios.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **radius-server template** *template-name*

The RADIUS server template view is displayed.

By default, the RADIUS server template named **default** is available on the device. This template can only be modified, but cannot be deleted.

**Step 3** Run **radius-server attribute translate**

The RADIUS attribute disabling and translation functions are enabled.

By default, the RADIUS attribute disabling and translation functions are disabled.

**Step 4** Run **radius-attribute disable** *attribute-name* { **receive** | **send** } *

A RADIUS attribute is disabled.

By default, no RADIUS attribute is disabled.

**Step 5** Configure the RADIUS attribute to be translated.

- **radius-attribute translate** *src-attribute-name dest-attribute-name* { **receive** | **send** | **access-accept** | **access-request** | **account-request** | **account-response** } *
- **radius-attribute translate extend vendor-specific** *src-vendor-id src-sub-id dest-attribute-name* { **access-accept** | **account-response** } *
- **radius-attribute translate extend** *src-attribute-name* **vendor-specific** *dest-vendor-id dest-sub-id* { **access-request** | **account-request** } *

By default, no RADIUS attribute is translated.

**----End**

## Verifying the Configuration

- Run the **display radius-attribute** [ **name** *attribute-name* | **type** { *attribute-number1* | **huawei** *attribute-number2* | **microsoft** *attribute-number3* | **dslforum** *attribute-number4* } ] command to check the RADIUS attributes supported by the device.
- Run the **display radius-attribute** [ **template** *template-name* ] **disable** command to check the disabled RADIUS attributes.
- Run the **display radius-attribute** [ **template** *template-name* ] **translate** command to check the RADIUS attribute translation configuration.

 Copyright © Huawei Technologies Co., Ltd. 

### 1.7.2.4.2 Configuring the RADIUS Attribute Check Function

## Context

After the RADIUS attribute check function is configured, the device checks whether the received RADIUS Access-Accept packets contain the specified attributes. If so, the device considers that authentication is successful; if not, the device considers that authentication fails and discards the packets.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **radius-server template** *template-name*

The RADIUS server template view is displayed.

By default, the RADIUS server template named **default** is available on the device. This template can only be modified, but cannot be deleted.

**Step 3** Run **radius-attribute check** *attribute-name*

The device is configured to check whether the received RADIUS Access-Accept packets contain the specified attribute.

By default, the device does not check whether RADIUS Access-Accept packets contain the specified attribute.

**----End**

### 1.7.2.4.3 Modifying the Value of a RADIUS Attribute

## Context

The value of the same RADIUS attribute may vary on RADIUS servers from different vendors. Therefore, RADIUS attribute values need to be modified, so that a Huawei device can successfully communicate with a third-party RADIUS server.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **radius-server template** *template-name*

The RADIUS server template view is displayed.

By default, the RADIUS server template named **default** is available on the device. This template can only be modified, but cannot be deleted.

**Step 3** Run **radius-attribute set** *attribute-name attribute-value* [ **auth-type mac** | **user-type ipsession** ]

The value of a RADIUS attribute is modified.

 Copyright © Huawei Technologies Co., Ltd. 

By default, values of RADIUS attributes are not modified.

**----End**

### 1.7.2.4.4 Configuring Standard RADIUS Attributes

## Context

For details about RADIUS attributes supported by the device, see **RADIUS Attributes**. The content or format of some standard RADIUS attributes can be configured.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **radius-server template** *template-name*

The RADIUS server template view is displayed.

By default, the RADIUS server template named **default** is available on the device. This template can only be modified, but cannot be deleted.

**Step 3** Configure standard RADIUS attributes.

- **Configure RADIUS attribute 4 (NAS-IP-Address) or 95 (NAS-IPv6-Address).**
  - Run **radius-attribute nas-ip** { *ip-address* | **ap-info** }

    RADIUS attribute 4 (NAS-IP-Address) is configured.

    By default, the source IP address of the NAS is the value of the NAS-IP-Address attribute.
  - Run **radius-attribute nas-ipv6** *ipv6-address*

    RADIUS attribute 95 (NAS-IPv6-Address) is configured.

    By default, the NAS-IPv6-Address attribute is not configured.
- **Configure RADIUS attribute 5 (NAS-Port).**
  a. Run **radius-server nas-port-format** { **new** | **old** }

     The format of the NAS port is configured.

     By default, the new NAS port format is used.

     When the new NAS port format is used, you can perform the following operation to configure the specific format.
  b. Run **radius-server format-attribute nas-port** *nas-port-sting*

     The new NAS port format is configured.

     By default, the default new NAS port format is used.
- **Configure RADIUS attribute 30 (Called-Station-Id).**
  a. Run **called-station-id mac-format** { **dot-split** | **hyphen-split** } [ **mode1** | **mode2** ] [ **lowercase** | **uppercase** ]

     Or run **called-station-id mac-format unformatted** [ **lowercase** | **uppercase** ]

 Copyright © Huawei Technologies Co., Ltd. 

The encapsulation format of the MAC address in the Called-Station-Id (30) attribute is configured.

By default, the MAC address format in the Called-Station-Id (30) attribute is XX-XX-XX-XX-XX-XX, in uppercase.

- **Configure RADIUS attribute 31 (Calling-Station-Id).**

  Run **calling-Station-Id mac-format** { **dot-split** | **hyphen-split** | **colon-split** } [ **mode1** | **mode2** ] [ **lowercase** | **uppercase** ]

  Or run **calling-Station-Id mac-format** { **unformatted** [ **lowercase** | **uppercase** ] | **bin** }

  The encapsulation format of the MAC address in the Calling-Station-Id (31) attribute is configured.

  By default, the MAC address format in the Calling-Station-Id (31) attribute is xxxx-xxxx-xxxx, in lowercase

- **Configure RADIUS attribute 32 (NAS-Identifier).**

  Run **radius-server nas-identifier-format** { **hostname** | **vlan-id** | **ap-info** }

  The encapsulation format of the NAS-Identifier attribute is configured.

  By default, the NAS-Identifier encapsulation format is the device's hostname.

- **Configure RADIUS attribute 80 (Message-Authenticator).**

  Run **radius-server attribute message-authenticator access-request**

  The device is configured to carry RADIUS attribute 80 (Message-Authenticator) in RADIUS authentication packets.

  By default, the device does not carry RADIUS attribute 80 (Message-Authenticator) in RADIUS authentication packets.

- **Configure RADIUS attribute 87 (NAS-Port-Id).**

  Run **radius-server nas-port-id-format** { **new** | **old** }

  The format of the NAS-Port-Id attribute is configured.

  By default, the new format of the NAS-Port-Id attribute is used.

**----End**

### 1.7.2.4.5 Configuring Huawei Proprietary RADIUS Attributes

## Context

For details about RADIUS attributes supported by the device, see **RADIUS Attributes**. The content or format of some Huawei proprietary RADIUS attributes can be configured.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **radius-server template** *template-name*

The RADIUS server template view is displayed.

By default, the RADIUS server template named **default** is available on the device. This template can only be modified, but cannot be deleted.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 3** Configure Huawei proprietary RADIUS attributes.

- Run **radius-server hw-ap-info-format include-ap-ip**

  The device is configured to carry the AP's IP address in Huawei proprietary attribute 26-141 (HW-AP-Information).

  By default, the device does not carry the AP's IP address in Huawei proprietary attribute 26-141 (HW-AP-Information).

**----End**

## 1.7.2.5 (Optional) Configuring Authorization Information

### 1.7.2.5.1 (Optional) Configuring a Service Scheme

## Context

Users must obtain authorization information before going online. You can configure a service scheme to manage authorization information about users.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **aaa**

The AAA view is displayed.

**Step 3** Run **service-scheme** *service-scheme-name*

A service scheme is created and the service scheme view is displayed.

By default, no service scheme is configured on the device.

**Step 4** Run **admin-user privilege level** *level*

The user is configured as the administrator and the administrator level for login is specified.

The value range of *level* is from 0 to 15. By default, the user level is not specified.

**Step 5** Configure server information.

| Step | Command | Remarks |
| --- | --- | --- |
| Configure a DHCP server group. | **dhcp-server group** *group-name* | By default, no DHCP server group is configured in a service scheme. |

 Copyright © Huawei Technologies Co., Ltd. 

| Step | Command | Remarks |
| --- | --- | --- |
| Configure the IP address of the primary DNS server. | **dns** *ip-address* | By default, no primary DNS server is configured in a service scheme. |
| Configure the IP address of the secondary DNS server. | **dns** *ip-address* **secondary** | By default, no secondary DNS server is configured in a service scheme. |

**Step 6** Configure resources delivered by the server in an Efficient VPN scenario.

| Step | Command | Remarks |
| --- | --- | --- |
| Configure the primary WINS server. | **wins** *ip-address* | By default, no primary WINS server is configured in a service scheme. |
| Configure the secondary WINS server. | **wins** *ip-address* **secondary** | By default, no secondary WINS server is configured in a service scheme. |
| Configure the URL and version number in the service scheme. | **auto-update url** *url-string* **version** *version-number* | By default, no URL or version number is configured in a service scheme. |
| Configure the default DNS domain name in the service scheme. | **dns-name** *domain-name* | By default, no default DNS domain name is configured in a service scheme. |

 Copyright © Huawei Technologies Co., Ltd. 

| Step | Command | Remarks |
| --- | --- | --- |
| Configure the local subnet information to be sent to the remote end. | **route set acl** *acl-number* | By default, no local subnet information is sent to the remote end. |
| Configure the IP address of the interface bound to the IPSec tunnel to be sent to the remote end. | **route set interface** | By default, no IP address of the interface bound to the IPSec tunnel is sent to the remote end. |

**Step 7** Run **ip-pool** *pool-name* [ **move-to** *new-position* ]

An IP address pool is bound to the service scheme or an existing IP address pool is moved.

By default, no IP address pool is bound to a service scheme.

NOTE

Ensure that the IP address pool has been configured before running this command.

**Step 8** Run **qos-profile** *profile-name*

A QoS profile is bound to the service scheme.

By default, no QoS profile is bound to a service scheme.

NOTE

Ensure that the QoS profile has been configured before running this command.

**Step 9** Run **idle-cut** *idle-time flow-value* [ **inbound** | **outbound** ]

The idle-cut function is enabled for domain users and the idle-cut parameters are set.

By default, the idle-cut function is disabled for domain users.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

The idle-cut function takes effect only after the idle time and traffic threshold are configured. To configure the traffic threshold, run the **idle-cut** *idle-time flow-value* command. To configure the idle time, use the value of *idle-time* configured on the device or the value (carried in RADIUS attribute 28 Idle-Timeout) authorized by the RADIUS server. If both values exist, the value authorized by the RADIUS server has a higher priority.

The **idle-cut** command configured in the service scheme view takes effect for administrators. For common users, the function takes effect only for PPPoE and Portal users.

**----End**

### 1.7.2.5.2 Configuring a User Group

## Context

Users must obtain authorization information before going online. You can configure a user group to manage authorization information about users.

## Procedure

- Configure a user group.

| Step | Command | Remarks |
| --- | --- | --- |
| Create a user group and enter the user group view. | **user-group** *group-name* | When using a user group in a two-node or dual-link HSB scenario, specify the user group index and ensure that the user group names and user group indexes configured on the active and standby devices are the same. |
| Bind an ACL to the user group. | **acl-id** *acl-number* | By default, no ACL is bound to a user group.<br>The IPv4 ACL bound to a user group must have been created using the **acl (system view)** command. |
| Configure the priority of the user group. | **remark** { **8021p** *8021p-value* \| **dscp** *dscp-value* \| **exp** *exp-value* \| **lp** *lp-value* }* | By default, the priority of a user group is not configured. |

**----End**

### 1.7.2.6 Creating and Configuring a Domain

## Context

A NAS performs domain-based user management. A domain is a group of users and each user belongs to a domain. A user uses only AAA configuration information in the domain to which the user belongs.

The device determines the domain to which a user belongs based on the user name. Before performing authentication, authorization, and accounting on users, you need to create the domain to which the users belong.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **aaa**

The AAA view is displayed.

**Step 3** Run **domain** *domain-name* [ **domain-index** *domain-index* ]

A domain is created and the domain view is displayed, or the view of an existing domain is displayed.

By default, the **default** and **default_admin** domains are available on the device. The **default** domain is used by common access users and the **default_admin** domain is used by administrators.

**Step 4** (Optional) Run **state** { **active** | **block** [ **time-range** *time-name* &<1-4> ] }

The domain state is configured.

By default, a domain is in active state after being created. When a domain is in blocking state, users in this domain cannot log in.

**Step 5** (Optional) Run **statistic enable**

Traffic statistics collection is enabled for users in the domain.

By default, traffic statistics collection is disabled for users in a domain.

**Step 6** (Optional) Configure the DNS function, which takes effect for all domains on the device.

1. Run **quit**

   Return to the AAA view.
2. Run **domainname-parse-direction** { **left-to-right** | **right-to-left** }

   The domain name resolution direction is configured.

   By default, a domain name is parsed from left to right.
3. Run **domain-name-delimiter** *delimiter*

   The domain name delimiter is configured.

   By default, the domain name delimiter is @.

 Copyright © Huawei Technologies Co., Ltd. 

4. Run **domain-location** { **after-delimiter** | **before-delimiter** }

   The position of a domain name is configured.

   By default, a domain name is placed behind the domain name delimiter.

NOTE

The DNS function can also be configured in the authentication profile view. If the DNS function is configured in both the AAA view and authentication profile view, the device preferentially uses the configuration in the authentication profile, which applies only to wireless users.

**Step 7** (Optional) Configure the security string function.

1. Run **security-name enable**

   The security string function is enabled.

   By default, the security string function is enabled.

2. Run **security-name-delimiter** *delimiter*

   The security string delimiter is configured.

   By default, the security string delimiter is an asterisk (*).

   NOTE

   The security string delimiter can also be configured in the authentication profile view. If the security string delimiter is configured in both the AAA view and authentication profile view, the device preferentially uses the configuration in the authentication profile, which applies only to wireless users.

**Step 8** (Optional) Specify a permitted domain for wireless users. (This step applies only to wireless users.)

| Procedure | Command | Description |
| --- | --- | --- |
| Return to the system view. | **quit** | - |
| Create an authentication profile and enter the authentication profile view. | **authentication-profile name** *authentication-profile-name* | By default, the device has six built-in authentication profiles: default_authen_profile, dot1x_authen_profile, mac_authen_profile, portal_authen_profile, dot1xmac_authen_profile, and multi_authen_profile. |

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | Command | Description |
| --- | --- | --- |
| Specify a permitted domain for wireless users. | **permit-domain name** *domain-name* &<1-4> | By default, no permitted domain is specified for wireless users.<br>After a permitted domain is specified in an authentication profile, only users in the permitted domain can be subject to authentication, authorization, and accounting. |

**----End**

## 1.7.2.7 Configuring Global Default Domains

### Context

The device determines the domain to which a user belongs based on the user name. If a user name does not contain a domain name, the device cannot determine the domain to which the user belongs, and adds the user to a global default domain. Based on user types (access users or administrators), global default domains are classified into the global default common domain and global default administrative domain.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Configure global default domains.

- Run **domain** *domain-name*

  The global default common domain is configured.
- Run **domain** *domain-name* **admin**

  The global default administrative domain is configured.

By default, two global default domains are available on the device: global default common domain named **default** and global default administrative domain named **default_admin**.

NOTE

The same domain name can be set for the global default common domain and global default administrative domain.

**----End**

### Verifying the Configuration of Global Default Domains

Run the **display aaa configuration** command to check the configuration of global default domains.

 Copyright © Huawei Technologies Co., Ltd. 

```
<Huawei> display aaa configuration
  Domain Name Delimiter            : @
  Domainname parse direction       : Left to right
  Domainname location              : After-delimiter
  Administrator user default domain: default_admin    //Global default administrative domain
  Normal user default domain       : default    //Global default common domain
```

## 1.7.2.8 Applying an AAA Scheme, a RADIUS Server Template, and Authorization Information to a Domain

### Context

AAA schemes, server templates, and authorization information are managed in a domain. A user uses only AAA configuration information in the domain to which the user belongs.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **aaa**

The AAA view is displayed.

**Step 3** Run **domain** *domain-name* [ **domain-index** *domain-index* ]

A domain is created and the domain view is displayed, or the view of an existing domain is displayed.

By default, the **default** and **default_admin** domains are available on the device. The **default** domain is used by common access users and the **default_admin** domain is used by administrators.

**Step 4** Run **authentication-scheme** *scheme-name*

An authentication scheme is applied to the domain.

By default, the authentication scheme named **default** is applied to the **default_admin** domain, and the authentication scheme named **radius** is applied to the **default** domain and other domains.

**Step 5** Run **accounting-scheme** *accounting-scheme-name*

An accounting scheme is applied to the domain.

By default, the **default** accounting scheme is applied to a domain. In the **default** accounting scheme, non-accounting is used and the real-time accounting function is disabled.

**Step 6** Run **radius-server** *template-name*

A RADIUS server template is applied to the domain.

By default, no RADIUS server template is applied to the **default_admin** domain, and the RADIUS server template named **default** is applied to the **default** domain and other domains.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 7** (Optional) Run **accounting-copy radius-server** *template-name*

The RADIUS accounting packet copy function is enabled, and a RADIUS server template for level-2 accounting is configured.

By default, the RADIUS accounting packet copy function is disabled.

NOTE

- Ensure that the IP address of the configured level-2 RADIUS accounting server must be different from that of the level-1 RADIUS accounting server (including the active/standby RADIUS accounting server).
- Ensure that the level-2 RADIUS accounting server template configured in the domain is different from the RADIUS server template for authentication and accounting in the domain. If they are the same, the **accounting-copy radius-server** command cannot be configured and the system displays an error message during the command configuration.

**Step 8** (Optional) Configure authorization information in the domain.

- Run **user-group** *group-name*

  A user group is applied to the domain. That is, the device will deliver authorization information of the user group to users in the domain.

  By default, no user group is applied to a domain.

- Run **service-scheme** *service-scheme-name*

  A service scheme is applied to the domain. That is, the device will deliver authorization information in the service scheme to users in the domain.

  By default, no service scheme is applied to a domain.

**----End**

## Verifying the Configuration

Run the **display domain** [ **name** *domain-name* ] command to check the domain configuration.

## 1.7.2.9 Configuring the RADIUS CoA or DM Function

## Context

The device supports the RADIUS CoA and DM functions. CoA provides a mechanism to change the rights of online users, and DM provides a mechanism to forcibly disconnect users.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Configure an authorization server.

 Copyright © Huawei Technologies Co., Ltd. 

| Step | Command | Remarks |
| --- | --- | --- |
| Configure a RADIUS authorization server. | **radius-server authorization** *ip-address* [ **vpn-instance** *vpn-instance-name* ] { **server-group** *group-name* **shared-key cipher** *key-string* \| **shared-key cipher** *key-string* [ **server-group** *group-name* ] } [ **ack-reserved-interval** *interval* ] [ **protect enable** ] | By default, no RADIUS authorization server is configured. |

**Step 3** (Optional) Run **radius-server authorization match-type** { **any** | **all** }

The device is configured to match RADIUS attributes in the received CoA or DM Request packets against user information on the device.

By default, a device matches RADIUS attributes in the received CoA or DM Request packets against user information on the device in **any** mode. That is, the device matches an attribute with a high priority in a Request packet against user information on the device.

**Step 4** (Optional) Run **radius-server session-manage** { *ip-address* [ **vpn-instance** *vpn-instance-name* ] **shared-key cipher** *share-key* | **any** }

Session management is enabled for the RADIUS server.

By default, session management is disabled for the RADIUS server.

**Step 5** (Optional) Configure the format of a RADIUS attribute to be parsed.

- Run **radius-server authorization calling-station-id decode-mac-format** { **bin** | **ascii** { **unformatted** | { **dot-split** | **hyphen-split** } [ **common** | **compress** ] } }

  The MAC address format in RADIUS attribute 31 (Calling-Station-Id) in RADIUS CoA or DM packets is configured.

  By default, the MAC address format in RADIUS attribute 31 (Calling-Station-Id) in RADIUS CoA or DM packets is xxxxxxxxxxxx, in lowercase.

- Run **radius-server authorization attribute-decode-sameastemplate**

  The device is configured to parse the MAC address format in RADIUS attribute 31 (Calling-Station-Id) in RADIUS CoA or DM packets based on RADIUS server template configurations.

  By default, the device is not configured to parse RADIUS attribute 31 in RADIUS CoA or DM packets based on RADIUS server template configurations.

  In a RADIUS server template, the MAC address format in RADIUS attribute 31 (Calling-Station-Id) is configured using the **calling-station-id mac-format** command.

**Step 6** (Optional) Configure the format of a RADIUS attribute to be encapsulated.

Run **radius-server authorization attribute-encode-sameastemplate**

The device is configured to encapsulate the attributes in RADIUS CoA or DM Response packets based on RADIUS server template configurations.

 Copyright © Huawei Technologies Co., Ltd. 

By default, the device is not configured to encapsulate the attributes in RADIUS CoA or DM Response packets based on RADIUS server template configurations.

Table 1-34 lists the RADIUS attributes that can be configured in this step.

**Table 1-34** Supported RADIUS attributes

| RADIUS Attribute | Description | Command for Configuring the Attribute in a RADIUS Server Template |
| --- | --- | --- |
| RADIUS attribute 1 (User-Name) | User name | **radius-server user-name domain-included** |
| RADIUS attribute 4 (NAS-IP-Address) | NAS IP address | **radius-attribute nas-ip** |
| RADIUS attribute 31 (Calling-Station-Id) | MAC address format | **calling-station-id mac-format** |

**Step 7** (Optional) Configure the update mode of user authorization information.

1. Run **aaa**

   The AAA view is displayed.

2. Run **authorization-modify mode** { **modify** | **overlay** }

   The update mode of user authorization information delivered by the authorization server is configured.

   By default, the update mode of user authorization information delivered by the authorization server is **overlay**.

**----End**

## Verifying the Configuration

Run the **display radius-server authorization configuration** command to check the RADIUS authorization server configuration.

## 1.7.2.10 Verifying the RADIUS AAA Configuration

## Procedure

- Run the **display aaa configuration** command to check the AAA summary.
- Run the **display authentication-scheme** [ *authentication-scheme-name* ] command to verify the authentication scheme configuration.
- Run the **display accounting-scheme** [ *accounting-scheme-name* ] command to verify the accounting scheme configuration.
- Run the **display service-scheme** [ **name** *name* ] command to verify the service scheme configuration.
- Run the **display radius-server configuration** [ **template** *template-name* ] command to verify the RADIUS server template configuration.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **display radius-server item** { **ip-address** { *ipv4-address* | *ipv6-address* } { **accounting** | **authentication** } | **template** *template-name* } command to verify the RADIUS server configuration.
- Run the **display radius-server** { **dead-interval** | **dead-count** } command to verify the specified RADIUS server detection interval and maximum number of consecutive unacknowledged packets.
- Run the **display radius-server authorization configuration** command to verify the RADIUS authorization server configuration.
- Run the **display radius-attribute** [ **name** *attribute-name* | **type** { *attribute-number1* | **huawei** *attribute-number2* | **microsoft** *attribute-number3* | **dslforum** *attribute-number4* } ] command to check the RADIUS attributes supported by the device.
- Run the **display radius-attribute** [ **template** *template-name* ] **disable** command to check the disabled RADIUS attributes.
- Run the **display radius-attribute** [ **template** *template-name* ] **translate** command to verify the setting for RADIUS attribute translation.
- Run the **display domain** [ **name** *domain-name* ] command to verify the domain configuration.
- Run the **display radius-server accounting-stop-packet** { **all** | **ip** { *ip-address* | *ipv6-address* } } command to verify the accounting-stop packets of the RADIUS server.
- Run the **display radius-attribute** [ **template** *template-name* ] **check** command to verify the to-be-tested attributes in RADIUS Access-Accept packets.
- Run the **display remote-user authen-fail** [ **blocked** | **username** *username* ] command to verify information about the accounts that fail in remote AAA authentication.
- Run the **display aaa statistics access-type-authenreq** command to display the number of authentication requests.
- Run the **display radius-server session-manage configuration** command to verify the session management configuration for the RADIUS server.

**----End**

# 1.7.3 Using HWTACACS to Perform Authentication, Authorization, and Accounting

## HWTACACS Authentication, Authorization, and Accounting

Similar to RADIUS, HWTACACS uses the client/server model to implement AAA for access users by communicating with the HWTACACS server.

HWTACACS protects a network from unauthorized access and supports command-line authorization. HWTACACS is more reliable in transmission and encryption than RADIUS, and is more suitable for security control.

 Copyright © Huawei Technologies Co., Ltd. 

## Configuration Procedure

### 1.7.3.1 Configuring an HWTACACS Server

If HWTACACS authentication and authorization are used, users' authentication, authorization, and accounting information needs to be configured on the HWTACACS server.

If a user wants to establish a connection with the access device through a network to obtain rights to access other networks and network resources, the access device transparently transmits the user's authentication, authorization, and accounting information to the HWTACACS server. The HWTACACS server determines whether the user can pass authentication based on the configured information. If the user passes the authentication, the RADIUS server sends an Access-Accept packet containing the user's authorization information to the access device. The access device then allows the user to access the network and grants rights to the user based on information in the Access-Accept packet.

### 1.7.3.2 Configuring AAA Schemes

#### Context

To use HWTACACS authentication, authorization, and accounting, set the authentication mode in the authentication scheme, authorization mode in the authorization scheme, and accounting mode in the accounting scheme to HWTACACS.

When configuring HWTACACS authentication, you can configure local authentication or non-authentication as the backup. This allows local authentication to be implemented if HWTACACS authentication fails. When configuring HWTACACS authorization, you can configure local authorization or non-authorization as the backup.

**NOTE**

If non-authentication is configured using the **authentication-mode** command, users can pass the authentication using any user name or password. To protect the device and improve network security, you are advised to enable authentication to allow only authenticated users to access the device or network.

#### Procedure

- Configure an authentication scheme.
  a. Run **system-view**

     The system view is displayed.
  b. Run **aaa**

     The AAA view is displayed.
  c. Run **authentication-scheme** *scheme-name*

     An authentication scheme is created and the authentication scheme view is displayed, or the view of an existing authentication scheme is displayed.

 Copyright © Huawei Technologies Co., Ltd. 

By default, two authentication schemes named **default** and **radius** are available on the device. These two authentication schemes can be modified but not deleted.

d. Run **authentication-mode hwtacacs**

The HWTACACS authentication mode is specified.

By default, local authentication is used.

To use local authentication as the backup, run the **authentication-mode hwtacacs** [ **local** ] command.

e. (Optional) Run **authentication-super** { **hwtacacs** | **super** } * [ **none** ]

The authentication mode for upgrading user levels is specified.

The default mode is **super** (local authentication).

f. Run **quit**

The AAA view is displayed.

g. (Optional) Configure the account locking function.

i. Run **remote-aaa-user authen-fail retry-interval** *retry-interval* **retry-time** *retry-time* **block-time** *block-time*

The remote AAA authentication account locking function is enabled, and the authentication retry interval, maximum number of consecutive authentication failures, and account locking period are configured.

By default, the remote AAA account locking function is enabled, the authentication retry interval is 300 minutes, the maximum number of consecutive authentication failures is 30, and the account locking period is 30 minutes.

ii. Run **aaa-quiet administrator except-list** { *ipv4-address* | *ipv6-address* } &<1-32>

A user is configured to access the network using a specified IP address if the user account is locked.

By default, a user cannot access the network if the user account is locked.

You can run the **display aaa-quiet administrator except-list** command to query the specified IP addresses.

iii. Run **remote-user authen-fail unblock** { **all** | **username** *username* }

A remote AAA authentication account that has failed authentication is unlocked.

h. (Optional) Run **security-name enable**

The security string function is enabled.

By default, the security string function is enabled.

i. (Optional) Run **domainname-parse-direction** { **left-to-right** | **right-to-left** }

The direction in which the user name and domain name are parsed is specified.

 Copyright © Huawei Technologies Co., Ltd. 

By default, a domain name is parsed from left to right.

j. Run **quit**

The system view is displayed.

k. (Optional) Run **aaa-authen-bypass enable time** *time-value*

The bypass authentication duration is set.

By default, the bypass authentication function is disabled.

- Configure an authorization scheme.
  a. Run **system-view**

  The system view is displayed.

  b. Run **aaa**

  The AAA view is displayed.

  c. Run **authorization-scheme** *authorization-scheme-name*

  An authorization scheme is created and the authorization scheme view is displayed, or the view of an existing authorization scheme is displayed.

  By default, an authorization scheme named **default** is available on the device. The **default** authorization scheme can be modified but not deleted.

  d. Run **authorization-mode hwtacacs** [ **local** ] [ **none** ]

  The authorization mode is specified.

  By default, local authorization is used.

  If HWTACACS authorization is configured, you must configure an HWTACACS server template and apply the template to the corresponding user domain.

  e. (Optional) Run **authorization-cmd** *privilege-level* **hwtacacs** [ **local** ] [ **none** ]

  Command-line authorization is enabled for users at a certain level.

  By default, command-line authorization is disabled for users at a certain level.

  If command-line authorization is enabled, you must configure an HWTACACS server template and apply the template to the corresponding user domain.

  f. Run **quit**

  The AAA view is displayed.

  g. Run **quit**

  The system view is displayed.

  h. (Optional) Run **aaa-author-bypass enable time** *time-value*

  The bypass authorization duration is set.

  By default, the bypass authorization is disabled.

 Copyright © Huawei Technologies Co., Ltd. 

i. (Optional) Run **aaa-author-cmd-bypass enable time** *time-value*

The bypass command-line authorization duration is set.

By default, the bypass command-line authorization is disabled.

- Configure an accounting scheme.
  a. Run **system-view**

  The system view is displayed.
  b. Run **aaa**

  The AAA view is displayed.
  c. Run **accounting-scheme** *accounting-scheme-name*

  An accounting scheme is created and the accounting scheme view is displayed, or the view of an existing accounting scheme is displayed.

  By default, the accounting scheme named **default** is available on the device. The **default** accounting scheme can be modified but not deleted.
  d. Run **accounting-mode hwtacacs**

  The hwtacacs accounting mode is specified.

  The default accounting mode is **none**.
  e. (Optional) Run **accounting start-fail** { **offline** | **online** }

  A policy for accounting-start failures is configured.

  By default, users cannot go online if accounting-start fails.
  f. (Optional) Run **accounting realtime** *interval*

  Real-time accounting is enabled and the accounting interval is set.

  By default, real-time accounting is disabled. The device performs accounting for users based on their online duration.
  g. (Optional) Run **accounting interim-fail** [ **max-times** *times* ] { **offline** | **online** }

  The maximum number of real-time accounting failures is set, and a policy is specified for the device if the maximum number of real-time accounting attempts fail.

  The default maximum number of real-time accounting failures is 3. The device will keep the users online if three real-time accounting attempts fail.

**----End**

## 1.7.3.3 Configuring an HWTACACS Server Template

## Context

When configuring an HWTACACS server template, you must specify the IP address, port number, and shared key of a specified HWTACACS server. Other settings, such as the HWTACACS user name format and traffic unit, have default values and can be modified based on network requirements.

 Copyright © Huawei Technologies Co., Ltd. 

The HWTACACS server template settings such as the HWTACACS user name format and shared key must be the same as those on the HWTACACS server.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **hwtacacs enable**

HWTACACS is enabled.

By default, HWTACACS is enabled.

**Step 3** Run **hwtacacs-server template** *template-name*

An HWTACACS server template is created and the HWTACACS server template view is displayed.

By default, no HWTACACS server template is configured on the device.

**Step 4** Configure HWTACACS authentication, authorization, and accounting servers.

| Configuration | Command | Description |
| --- | --- | --- |
| Configure an HWTACACS authentication server. | • Configure an IPv4 server: **hwtacacs-server authentication** *ipv4-address* [ *port* ] [ **public-net** \| **vpn-instance** *vpn-instance-name* ] [ **secondary** \| **third** ] [ **shared-key cipher** *key-string* ]<br>• Configure an IPv6 server: **hwtacacs-server authentication** *ipv6-address* [ *port* ] [ **public-net** ] [ **secondary** \| **third** ] [ **shared-key cipher** *key-string* ] | By default, no HWTACACS authentication server is configured. |

 Copyright © Huawei Technologies Co., Ltd. 

| Configuration | Command | Description |
| --- | --- | --- |
| Configure an HWTACACS authorization server. | • Configure an IPv4 server: **hwtacacs-server authorization** *ipv4-address* [ *port* ] [ **public-net** \| **vpn-instance** *vpn-instance-name* ] [ **secondary** \| **third** ] [ **shared-key cipher** *key-string* ]<br>• Configure an IPv6 server: **hwtacacs-server authorization** *ipv6-address* [ *port* ] [ **public-net** ] [ **secondary** \| **third** ] [ **shared-key cipher** *key-string* ] | By default, no HWTACACS authorization server is configured. |
| Configure an HWTACACS accounting server. | • Configure an IPv4 server: **hwtacacs-server accounting** *ipv4-address* [ *port* ] [ **public-net** \| **vpn-instance** *vpn-instance-name* ] [ **secondary** \| **third** ] [ **shared-key cipher** *key-string* ]<br>• Configure an IPv6 server: **hwtacacs-server accounting** *ipv6-address* [ *port* ] [ **public-net** ] [ **secondary** \| **third** ] [ **shared-key cipher** *key-string* ] | By default, no HWTACACS accounting server is configured. |

**Step 5** Set parameters for interconnection between the device and an HWTACACS server.

| Procedure | | | Command | Description |
| --- | --- | --- | --- | --- |
| Set the shared key for th | System view | Return to the system view. | **quit** | - |

| Procedure | | | Command | Description |
| --- | --- | --- | --- | --- |
| e HWTACACS server. | | Set the shared key for the HWTACACS server. | **hwtacacs-server shared-key cipher** *key-string* | By default, no shared key is set for an HWTACACS server. |
| | | Enter the HWTACACS server template view. | **hwtacacs-server template** *template-name* | - |
| | HWTACACS server template view | | **hwtacacs-server shared-key cipher** *key-string* | By default, no shared key is set for an HWTACACS server. |
| (Optional) Configure the format of the user name in the packet sent by the device to the HWTACACS server. | | | • Configure the user name to contain the domain name: **hwtacacs-server user-name domain-included**<br>• Configure the original user name: **hwtacacs-server user-name original**<br>• Configure the user name not to contain the domain name: **undo hwtacacs-server user-name domain-included** | By default, the device does not change the user name entered by the user when sending packets to the HWTACACS server. |
| (Optional) Set the HWTACACS traffic unit. | | | **hwtacacs-server traffic-unit** { **byte** \| **kbyte** \| **mbyte** \| **gbyte** } | The default HWTACACS traffic unit on the device is bytes. |

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | Command | Description |
| --- | --- | --- |
| (Optional) Set the source IP address for communication between the device and HWTACACS server. | **hwtacacs-server source-ip** { *ip-address* \| **source-loopback** *interface-number* }<br>or **hwtacacs-server source-ipv6** { *ipv6-address* \| **source-loopback** *interface-number* } | By default, the device uses the IP address of the actual outbound interface as the source IP address encapsulated in HWTACACS packets. |

**Step 6** (Optional) Set the response timeout interval and activation interval for the HWTACACS server.

| Procedure | Command | Description |
| --- | --- | --- |
| Set the response timeout interval for the HWTACACS server. | **hwtacacs-server timer response-timeout** *interval* | The default response timeout interval for an HWTACACS server is 5 seconds.<br>If the device does not receive a response packet from an HWTACACS server within the response timeout interval, it considers that the HWTACACS server is unreachable and then tries other authentication and authorization methods. |
| Set the interval for the primary HWTACACS server to restore to the active state. | **hwtacacs-server timer quiet** *interval* | The default interval for the primary HWTACACS server to restore to the active state is 5 minutes. |

**Step 7** Run **quit**

The system view is displayed.

**Step 8** (Optional) Run **hwtacacs-server accounting-stop-packet resend** { **disable** | **enable** *number* }

Retransmission of accounting-stop packets is enabled and the number of packets that can be retransmitted each time is specified.

By default, retransmission of accounting-stop packets is enabled, and 100 account-stop packets can be retransmitted each time.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 9** Run **return**

The user view is displayed.

**Step 10** (Optional) Run **hwtacacs-user change-password hwtacacs-server** *template-name*

The password saved on the HWTACACS server is changed.

NOTE

To ensure device security, you are advised to frequently change the password.

**Step 11** (Optional) Run **test-aaa** *user-name user-password* **hwtacacs-template** *template-name* [ **accounting** [ **start** | **realtime** | **stop** ] ]

Connectivity between the device and authentication or accounting server is tested. If the user passes the HWTACACS authentication or accounting, the device is properly connected to the authentication or accounting server.

**----End**

## 1.7.3.4 (Optional) Configuring a Recording Scheme

## Context

Improper operations by a network administrator may sometimes cause a network failure. After HWTACACS authentication and authorization are configured, the server can record administrator's operations. These records can be used to locate the problem if a network failure occurs.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **aaa**

The AAA view is displayed.

**Step 3** Run **recording-scheme** *recording-scheme-name*

A recording scheme is created and the recording scheme view is displayed.

By default, no recording scheme is configured on the device.

**Step 4** Run **recording-mode hwtacacs** *template-name*

The recording scheme is associated with the HWTACACS server template.

By default, a recording scheme is not associated with any HWTACACS server template.

**Step 5** Run **quit**

The AAA view is displayed.

**Step 6** Run **cmd recording-scheme** *recording-scheme-name*

 Copyright © Huawei Technologies Co., Ltd. 

A policy is configured to record the commands that have been executed on the device.

By default, the commands used on the device are not recorded.

**Step 7** Run **outbound recording-scheme** *recording-scheme-name*

A policy is configured to record connection information.

By default, connection information is not recorded.

**Step 8** Run **system recording-scheme** *recording-scheme-name*

A policy is configured to record system events.

By default, system events are not recorded.

**----End**

## 1.7.3.5 (Optional) Configuring a Service Scheme

## Context

Users must obtain authorization information before going online. You can configure a service scheme to manage authorization information about users.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **aaa**

The AAA view is displayed.

**Step 3** Run **service-scheme** *service-scheme-name*

A service scheme is created and the service scheme view is displayed.

By default, no service scheme is configured on the device.

**Step 4** Run **admin-user privilege level** *level*

The user is configured as the administrator and the administrator level for login is specified.

The value range of *level* is from 0 to 15. By default, the user level is not specified.

**Step 5** Configure server information.

| Step | Command | Remarks |
| --- | --- | --- |
| Configure a DHCP server group. | **dhcp-server group** *group-name* | By default, no DHCP server group is configured in a service scheme. |

 Copyright © Huawei Technologies Co., Ltd. 

| Step | Command | Remarks |
| --- | --- | --- |
| Configure the IP address of the primary DNS server. | **dns** *ip-address* | By default, no primary DNS server is configured in a service scheme. |
| Configure the IP address of the secondary DNS server. | **dns** *ip-address* **secondary** | By default, no secondary DNS server is configured in a service scheme. |

**Step 6** Configure resources delivered by the server in an Efficient VPN scenario.

| Step | Command | Remarks |
| --- | --- | --- |
| Configure the primary WINS server. | **wins** *ip-address* | By default, no primary WINS server is configured in a service scheme. |
| Configure the secondary WINS server. | **wins** *ip-address* **secondary** | By default, no secondary WINS server is configured in a service scheme. |
| Configure the URL and version number in the service scheme. | **auto-update url** *url-string* **version** *version-number* | By default, no URL or version number is configured in a service scheme. |
| Configure the default DNS domain name in the service scheme. | **dns-name** *domain-name* | By default, no default DNS domain name is configured in a service scheme. |

 Copyright © Huawei Technologies Co., Ltd. 

| Step | Command | Remarks |
| --- | --- | --- |
| Configure the local subnet information to be sent to the remote end. | **route set acl** *acl-number* | By default, no local subnet information is sent to the remote end. |
| Configure the IP address of the interface bound to the IPSec tunnel to be sent to the remote end. | **route set interface** | By default, no IP address of the interface bound to the IPSec tunnel is sent to the remote end. |

**Step 7** Run **ip-pool** *pool-name* [ **move-to** *new-position* ]

An IP address pool is bound to the service scheme or an existing IP address pool is moved.

By default, no IP address pool is bound to a service scheme.

NOTE

Ensure that the IP address pool has been configured before running this command.

**Step 8** Run **qos-profile** *profile-name*

A QoS profile is bound to the service scheme.

By default, no QoS profile is bound to a service scheme.

NOTE

Ensure that the QoS profile has been configured before running this command.

**Step 9** Run **idle-cut** *idle-time flow-value* [ **inbound** | **outbound** ]

The idle-cut function is enabled for domain users and the idle-cut parameters are set.

By default, the idle-cut function is disabled for domain users.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

The idle-cut function takes effect only after the idle time and traffic threshold are configured. To configure the traffic threshold, run the **idle-cut** *idle-time flow-value* command. To configure the idle time, use the value of *idle-time* configured on the device or the value (carried in RADIUS attribute 28 Idle-Timeout) authorized by the RADIUS server. If both values exist, the value authorized by the RADIUS server has a higher priority.

The **idle-cut** command configured in the service scheme view takes effect for administrators. For common users, the function takes effect only for PPPoE and Portal users.

**----End**

## 1.7.3.6 Applying AAA Schemes to a Domain

## Context

The created authentication scheme, authorization scheme, accounting scheme, and HWTACACS server template are in effect only when they are applied to a domain.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **aaa**

The AAA view is displayed.

**Step 3** Run **domain** *domain-name* [ **domain-index** *domain-index* ]

A domain is created and the domain view is displayed, or the view of an existing domain is displayed.

The device has two default domains:

- **default**: Used by common access users
- **default_admin**: Used by administrators

NOTE

- If a user enters a user name that does not contain a domain name, the user is authenticated in the default domain. In this case, you need to run the **domain** *domain-name* [ **admin** ] command and set *domain-name* to configure a global default domain on the device.
- If a user enters a user name that contains a domain name during authentication, the user must enter the correct value of *domain-name*.

**Step 4** Apply AAA schemes to the domain.

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | Command | Description |
| --- | --- | --- |
| Apply an authentication scheme to the domain. | **authentication-scheme** *scheme-name* | By default, the authentication scheme **default** is applied to the **default_admin** domain, and the authentication scheme named **radius** is applied to the **default** domain and other domains. |
| Apply an authorization scheme to the domain. | **authorization-scheme** *authorization-scheme-name* | By default, no authorization scheme is applied to a domain. |
| Apply an accounting scheme to the domain. | **accounting-scheme** *accounting-scheme-name* | By default, the accounting scheme **default** is applied to a domain. In this accounting scheme, non-accounting is used and real-time accounting is disabled. |

**Step 5** Apply a service scheme and an HWTACACS server template to the domain.

| Procedure | Command | Description |
| --- | --- | --- |
| (Optional) Apply a service scheme to the domain. | **service-scheme** *service-scheme-name* | By default, no service scheme is applied to a domain. |
| Apply an HWTACACS server template to the domain. | **hwtacacs-server** *template-name* | By default, no HWTACACS server template is applied to a domain. |

**Step 6** (Optional) Configure other functions for the domain.

| Procedure | Command | Description |
| --- | --- | --- |
| Specify the domain state. | **state** { **active** \| **block** [ **time-range** *time-name* &<1–4> ] } | When a domain is in the blocking state, users in this domain cannot log in. By default, a created domain is in the active state. |

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | Command | Description |
| --- | --- | --- |
| Apply a user group to the domain. | **user-group** *group-name* | By default, no user group is applied to a domain. |

**Step 7** (Optional) Run **statistic enable**

Traffic statistics collection is enabled for users in the domain.

By default, traffic statistics collection is disabled for users in a domain.

**Step 8** (Optional) Configure a domain name parsing scheme. (If domain name parsing is configured in both the AAA view and authentication profile view, the device preferentially uses the configuration in the authentication profile. The configuration in the authentication profile applies only to wireless users.)

| Procedure | | Command | Description |
| --- | --- | --- | --- |
| AAA view | Exit from the domain view. | **quit** | - |
| | Specify the domain name parsing direction. | **domainname-parse-direction** { **left-to-right** \| **right-to-left** } | The domain name can be parsed from left to right, or from right to left.<br>By default, the domain name is parsed from left to right. |
| | Set the domain name delimiter. | **domain-name-delimiter** *delimiter* | A domain name delimiter can be any of the following: \ / : < > \| @ ' %.<br>The default domain name delimiter is @. |
| | Specify the domain name location. | **domain-location** { **after-delimiter** \| **before-delimiter** } | The domain name can be placed before or after the delimiter.<br>By default, the domain name is placed after the domain name delimiter. |

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | | Command | Description |
| --- | --- | --- | --- |
| | Set the security string delimiter. | **security-name-delimiter** *delimiter* | The default security string delimiter is * (asterisk). |

**----End**

### 1.7.3.7 Verifying the HWTACACS AAA Configuration

## Procedure

- Run the **display aaa configuration** command to check the AAA summary.
- Run the **display authentication-scheme** [ *authentication-scheme-name* ] command to verify the authentication scheme configuration.
- Run the **display authorization-scheme** [ *authorization-scheme-name* ] command to verify the authorization scheme configuration.
- Run the **display accounting-scheme** [ *accounting-scheme-name* ] command to verify the accounting scheme configuration.
- Run the **display recording-scheme** [ *recording-scheme-name* ] command to verify the recording scheme configuration.
- Run the **display service-scheme** [ **name** *name* ] command to verify the service scheme configuration.
- Run the **display hwtacacs-server template** [ *template-name* ] command to verify the HWTACACS server template configuration.
- Run the **display hwtacacs-server template** *template-name* **verbose** command to check statistics about HWTACACS authentication, accounting, and authorization.
- Run the **display hwtacacs-server accounting-stop-packet** { **all** | *number* | **ip** { *ipv4-address* | *ipv6-address* } } command to verify information about accounting-stop packets of the HWTACACS server.
- Run the **display domain** [ **name** *domain-name* ] command to verify the domain configuration.
- Run the **display aaa statistics access-type-authenreq** command to display the number of authentication requests.

**----End**

# 1.7.4 Configuring HACA Authentication

## HACA Authentication

Two authentication methods are available in cloud-based management scenario: 802.1X authentication and Portal authentication. In 802.1X authentication, the

 Copyright © Huawei Technologies Co., Ltd. 

device must be connected to a third-party RADIUS server. Portal authentication is more often used in cloud-based management. The authentication server is located on the cloud, so packets between the device and server must traverse the NAT device. However, Portal protocol packets cannot traverse the NAT device. HACA implements communication between the device and server, and then Portal authentication can be performed.

Similar to the RADIUS protocol, the HACA protocol uses the client/server model to authenticate access users.

## Configuration Procedure

## 1.7.4.1 Configuring an HACA Server

## Context

When HACA authentication and authorization are used, the authentication and authorization information must be configured on the HACA server.

When a user requests to access the Internet, the access device forwards authentication information to the HACA server. The HACA server then decides whether to allow the user to pass based on the configured information. If the user is allowed, the HACA server sends an access-accept message carrying authorization information to the access device. The access device then authorizes network access rights to the user according to the access-accept message.

## 1.7.4.2 Configuring an AAA Scheme

## Context

If HACA authentication and authorization are used, set the authentication mode in the authentication scheme to HACA and the accounting mode in an accounting scheme to HACA.

NOTE

If non-authentication is configured using the **authentication-mode** command, users can pass the authentication using any user name or password. To protect the device and improve network security, you are advised to enable authentication to allow only authenticated users to access the device or network.

## Procedure

- Configure an authentication scheme.
  a. Run **system-view**

     The system view is displayed.
  b. Run **aaa**

     The AAA view is displayed.
  c. Run **authentication-scheme** *scheme-name*

 Copyright © Huawei Technologies Co., Ltd. 

An authentication scheme is created and its view is displayed, or the view of an existing authentication scheme is displayed.

By default, two authentication schemes named **default** and **radius** are available on the device. The two authentication schemes can be modified but not deleted.

d. Run **authentication-mode haca**

The authentication method is set to HACA.

By default, local authentication is used.

To use local authentication as the backup authentication mode, run the **authentication-mode haca local** command to configure local authentication.

NOTE

If multiple authentication modes are configured in an authentication scheme, the authentication modes are used according to the sequence in which they were configured. The device uses the authentication mode that was configured later only when it does not receive any response from the current authentication. The device stops the authentication if the current authentication fails.

e. Run **quit**

Return to the AAA view.

f. (Optional) Configure the account locking function.

i. Run **remote-aaa-user authen-fail retry-interval** *retry-interval* **retry-time** *retry-time* **block-time** *block-time*

The remote AAA authentication account locking function is enabled, and the authentication retry interval, maximum number of consecutive authentication failures, and account locking period are configured.

By default, the remote AAA account locking function is enabled, the authentication retry interval is 300 minutes, the maximum number of consecutive authentication failures is 30, and the account locking period is 30 minutes.

ii. Run **aaa-quiet administrator except-list** { *ipv4-address* | *ipv6-address* } &<1-32>

A user is configured to access the network using a specified IP address if the user account is locked.

By default, a user cannot access the network if the user account is locked.

You can run the **display aaa-quiet administrator except-list** command to query the specified IP addresses.

iii. Run **remote-user authen-fail unblock** { **all** | **username** *username* }

A remote AAA authentication account that has failed authentication is unlocked.

g. (Optional) Run **domainname-parse-direction** { **left-to-right** | **right-to-left** }

The direction in which the domain name is parsed is configured.

 Copyright © Huawei Technologies Co., Ltd. 

By default, the domain name is parsed from left to right.

h. (Optional) Run **aaa-author session-timeout invalid-value enable**

The device will not disconnect or reauthenticate users when the RADIUS server delivers session-timeout with value 0.

By default, the device disconnects or reauthenticates users when the RADIUS server delivers session-timeout with value 0.

i. Run **quit**

Return to the system view.

- Configuring an accounting scheme

a. Run **system-view**

The system view is displayed.

b. Run **aaa**

The AAA view is displayed.

c. Run **accounting-scheme** *accounting-scheme-name*

An accounting scheme is created, and the corresponding accounting scheme view or an existing accounting scheme view is displayed.

There is a default accounting scheme named **default** on the device. This default accounting scheme can be modified but not deleted.

d. Run **accounting-mode haca**

The haca accounting mode in an accounting scheme is configured.

By default, the accounting mode is **none**.

e. (Optional) Run **accounting start-fail** { **offline** | **online** }

A policy for accounting-start failures is configured.

By default, users cannot go online if accounting-start fails.

f. (Optional) Run **accounting realtime** *interval*

Real-time accounting is enabled and the interval for real-time accounting is set.

By default, the device performs accounting based on user online duration, the real-time accounting function is disabled.

g. (Optional) Run **accounting interim-fail** [ **max-times** *times* ] { **offline** | **online** }

The maximum number of real-time accounting failures is set and a policy used after the number of real-time accounting failures exceeds the maximum is configured.

By default, the maximum number of real-time accounting failures is 3 and the device keeps users online after the number of real-time accounting failures exceeds the maximum.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

### 1.7.4.3 Configuring an HACA Server Template

## Context

In an HACA server template, specify the server IP address and port number. Other settings such as the HACA user name format and HACA server response timeout have default values and can be changed based on network requirements.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **haca-server template** *template-name*

An HACA server template is created and its view is displayed.

By default, no HACA server template exists on the device.

**Step 3** Run **haca-server server-address** *ip-address* [ *port* ] *pki-realm-name*

The IP address and port number for the HACA server are configured.

By default, the IP address and port number of the HACA server are not configured on the device.

**Step 4** Run the following commands as required:

- To add the domain name to the user name in the packets sent to the HACA server, run the **haca-server user-name domain-included** command.
- To retain the original user name in the packets sent to the HACA server, run the **haca-server user-name original** command.

By default, the device does not modify the user name entered by the user in the packets sent to the HACA server.

**Step 5** Run **haca-server source-ip** *ip-address*

The source IP address is specified for HACA packets.

By default, no source IP address is specified for HACA packets. The device uses the IP address of the actual outbound interface as the source IP address of HACA packets.

**Step 6** (Optional) Run **haca-server timer response-timeout** *interval*

The response timeout interval for the HACA server is set.

By default, the timeout duration of the HACA server is 5 seconds.

**Step 7** (Optional) Run **haca-server timer down-delay** *interval*

The delay after which an HACA server is disconnected is set.

By default, the delay after which an HACA server is disconnected is 30 seconds.

**Step 8** (Optional) Run **haca-server timer reconnection** *interval*

The interval for reconnecting to the HACA server is set.

 Copyright © Huawei Technologies Co., Ltd. 

By default, the interval for reconnecting to the HACA server is one minute.

**Step 9** (Optional) Run **haca-server timer heart-beat** *interval*

The heartbeat interval is set.

By default, the heartbeat interval is 5 minutes.

**Step 10** (Optional) Run **haca-server accounting-stop-packet resend** [ *resend-times* ]

Retransmission of accounting-stop packets is enabled, and the number of accounting-stop packets that can be retransmitted is set.

By default, three accounting-stop packets can be retransmitted.

**Step 11** Run **haca enable**

HACA is enabled.

By default, HACA is disabled.

**Step 12** Run **quit**

Return to the system view.

**Step 13** (Optional) Run **haca-server timer user-syn** *interval*

The interval for synchronizing user information to the HACA server is set.

By default, the interval for synchronizing user information to the HACA server is 10 minutes.

**----End**

## 1.7.4.4 (Optional) Configuring a Service Scheme

## Context

Users must obtain authorization information before going online. You can configure a service scheme to manage authorization information about users.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **aaa**

The AAA view is displayed.

**Step 3** Run **service-scheme** *service-scheme-name*

A service scheme is created and the service scheme view is displayed.

By default, no service scheme is configured on the device.

**Step 4** Run **admin-user privilege level** *level*

The user is configured as the administrator and the administrator level for login is specified.

 Copyright © Huawei Technologies Co., Ltd. 

The value range of *level* is from 0 to 15. By default, the user level is not specified.

**Step 5** Configure server information.

| Step | Command | Remarks |
| --- | --- | --- |
| Configure a DHCP server group. | **dhcp-server group** *group-name* | By default, no DHCP server group is configured in a service scheme. |
| Configure the IP address of the primary DNS server. | **dns** *ip-address* | By default, no primary DNS server is configured in a service scheme. |
| Configure the IP address of the secondary DNS server. | **dns** *ip-address* **secondary** | By default, no secondary DNS server is configured in a service scheme. |

**Step 6** Configure resources delivered by the server in an Efficient VPN scenario.

| Step | Command | Remarks |
| --- | --- | --- |
| Configure the primary WINS server. | **wins** *ip-address* | By default, no primary WINS server is configured in a service scheme. |
| Configure the secondary WINS server. | **wins** *ip-address* **secondary** | By default, no secondary WINS server is configured in a service scheme. |
| Configure the URL and version number in the service scheme. | **auto-update url** *url-string* **version** *version-number* | By default, no URL or version number is configured in a service scheme. |

 Copyright © Huawei Technologies Co., Ltd. 

| Step | Command | Remarks |
| --- | --- | --- |
| Configure the default DNS domain name in the service scheme. | **dns-name** *domain-name* | By default, no default DNS domain name is configured in a service scheme. |
| Configure the local subnet information to be sent to the remote end. | **route set acl** *acl-number* | By default, no local subnet information is sent to the remote end. |
| Configure the IP address of the interface bound to the IPSec tunnel to be sent to the remote end. | **route set interface** | By default, no IP address of the interface bound to the IPSec tunnel is sent to the remote end. |

**Step 7** Run **ip-pool** *pool-name* [ **move-to** *new-position* ]

An IP address pool is bound to the service scheme or an existing IP address pool is moved.

By default, no IP address pool is bound to a service scheme.

NOTE

Ensure that the IP address pool has been configured before running this command.

**Step 8** Run **qos-profile** *profile-name*

A QoS profile is bound to the service scheme.

By default, no QoS profile is bound to a service scheme.

NOTE

Ensure that the QoS profile has been configured before running this command.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 9** Run **idle-cut** *idle-time flow-value* [ **inbound** | **outbound** ]

The idle-cut function is enabled for domain users and the idle-cut parameters are set.

By default, the idle-cut function is disabled for domain users.

NOTE

The idle-cut function takes effect only after the idle time and traffic threshold are configured. To configure the traffic threshold, run the **idle-cut** *idle-time flow-value* command. To configure the idle time, use the value of *idle-time* configured on the device or the value (carried in RADIUS attribute 28 Idle-Timeout) authorized by the RADIUS server. If both values exist, the value authorized by the RADIUS server has a higher priority.

The **idle-cut** command configured in the service scheme view takes effect for administrators. For common users, the function takes effect only for PPPoE and Portal users.

**----End**

## 1.7.4.5 Applying an AAA Scheme to a Domain

## Context

The created authentication scheme and HACA server template take effect only after being applied to a domain.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **aaa**

The AAA view is displayed.

**Step 3** Run **domain** *domain-name*

A domain is created and the domain view is displayed, or the view of an existing domain is displayed.

The device has two default domains named **default** and **default_admin**. The two domains can be modified but not deleted.

**Step 4** Run **authentication-scheme** *authentication-scheme-name*

An authentication scheme is applied to the domain.

By default, the authentication scheme named **radius** is applied to the **default** domain, the authentication scheme named **default** is applied to the **default_admin** domain, and the authentication scheme named **radius** is applied to other domains.

**Step 5** Run **accounting-scheme** *accounting-scheme-name*

An accounting scheme is applied to the domain.

 Copyright © Huawei Technologies Co., Ltd. 

By default, the accounting scheme named **default** is applied to a domain. In this default accounting scheme, non-accounting is used and the real-time accounting function is disabled.

**Step 6** Run **service-scheme** *service-scheme-name*

A service scheme is applied to the domain.

By default, no service scheme is bound to a domain.

**Step 7** Run **haca-server** *template-name*

An HACA server template is applied to the domain.

By default, no HACA server template is applied to a domain.

**Step 8** (Optional) Run **state** { **active** | **block** [ **time-range** *time-name* &<1–4> ] }

The domain status is configured.

By default, a domain is in active state after being created. When a domain is in blocking state, users in this domain cannot log in.

**Step 9** (Optional) Configure a domain name resolution scheme. (If domain name resolution is configured in both the AAA view and authentication profile view, the device preferentially uses the configuration in the authentication profile. The configuration in the authentication profile applies only to wireless users.)

| Procedure | | Command | Description |
| --- | --- | --- | --- |
| AAA view | Exit from the domain view. | **quit** | - |
| | Configure the domain name resolution direction. | **domainname-parse-direction** { **left-to-right** \| **right-to-left** } | The domain name can be resolved from left to right, or from right to left.<br>By default, the domain name is resolved from left to right. |
| | Configure a domain name delimiter. | **domain-name-delimiter** *delimiter* | A domain name delimiter can be any of the following: \ / : < > \| @ ' %.<br>The default domain name delimiter is @. |

 Copyright © Huawei Technologies Co., Ltd. 

| Procedure | | Command | Description |
| --- | --- | --- | --- |
| | Configure the domain name location. | **domain-location** { **after-delimiter** \| **before-delimiter** } | By default, the domain name is placed after the domain name delimiter. |
| | Configure a security string delimiter. | **security-name-delimiter** *delimiter* | By default, the security string delimiter is an asterisk (*). |

**----End**

### 1.7.4.6 Verifying the HACA Authentication Configuration

#### Procedure

- Run the **display haca-server configuration** [ **template** *template-name* ] command to check the HACA server template configuration.
- Run the **display haca-server statistics** { **all** | **message** | **packet** [ **authentication** | **authorization** | **accounting** | **cut-notify** | **cut-request** | **register** | **user-syn** ] } [ **template** *template-name* ] command to check HACA packet statistics.
- Run the **display haca-server accounting-stop-packet all** command to view information about all accounting-stop packets on the HACA server.

**----End**

## 1.8 Maintaining AAA

### 1.8.1 Forcing Users to Go Offline

#### Context

You can force online users to go offline by specifying the domain name or interface. This function is applicable to situations such as when the online users are unauthorized, the number of online users reaches the maximum, or the AAA configurations are modified. For example, when you modify the AAA configurations of online users, the new AAA configurations take effect on these users only after you force them to go offline.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

- If you delete the AAA configuration of online users, the users may be forced to go offline.

## Procedure

- Run the **cut access-user** { **domain** *domain-name* | **interface** *interface-type interface-number* [ **vlan** *vlan-id* [ **qinq** *qinq-vlan-id* ] ] | **ip-address** *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **mac-address** *mac-address* | **service-scheme** *service-scheme-name* | **access-slot** *slot-id* | **ssid** *ssid-name* | **user-group** *group-number* | **user-id** *begin-number* [ *end-number* ] | **username** *user-name* } or **cut access-user access-type** { **admin** [ **ftp** | **ssh** | **telnet** | **terminal** | **web** ] | **ppp** | **l2tp** } [ **username** *user-name* ] command in the AAA view to disconnect one or more sessions. After a session of a user is disconnected, the user is forced to go offline.

**----End**

# 1.8.2 Testing Whether a User Can Pass RADIUS Authentication or Accounting

## Prerequisites

RADIUS authentication or accounting is configured.

NOTE

If HWTACACS authentication or accounting is configured, you can run the **test-aaa** *user-name user-password* **hwtacacs-template** *template-name* [ **accounting** [ **start** | **realtime** | **stop** ] ] commands to test connectivity between the device and authentication server or accounting server.

## Context

Test whether a user can pass RADIUS authentication or accounting, helping the administrator locate faults.

## Procedure

- Run the **test-aaa** *user-name user-password* **radius-template** *template-name* [ **chap** | **pap** | **accounting** [ **start** | **realtime** | **stop** ] ] command in any view to test whether a user can pass RADIUS authentication or accounting.

**----End**

## Follow-up Procedure

- The **test-aaa** command returns an account test timeout message.

  RADIUS authentication test for a single user times out.

  ```
  <Huawei> test-aaa user1 huawei123 radius-template huawei
  Info: Account test time out.
  ```

  RADIUS accounting test for a single user times out.

  ```
  <Huawei> test-aaa user1 huawei123 radius-template huawei accounting
  Info: Account test time out.
  ```

 Copyright © Huawei Technologies Co., Ltd. 

  - The possible causes are as follows:
    - The route between the device and the server is unreachable.
    - The NAS-IP in the RADIUS server template is different from the NAS-IP configured on the RADIUS server.
    - The authentication or accounting port in the RADIUS server template is incorrect.
    - The authentication or accounting port on the RADIUS server is occupied by another application.
    - The RADIUS server address in the RADIUS server template is incorrect.
    - The IP address of the access control device is incorrect or the RADIUS server is not started.
  - Handling procedure:
    - Run the **ping** command to check whether a reachable route exists between the device and the server. If there is no reachable route, establish a static route or use a routing protocol to establish a dynamic route between the device and the server.
    - Run the **display radius-server configuration** [ **template** *template-name* ] command in any view to check whether the port number and NAS-IP in the RADIUS server template are the same as those on the RADIUS server. If they are not the same, configure the same port number and NAS-IP.
    - Check whether the authentication and accounting port numbers on the RADIUS server are 1812 and 1813, respectively. If not, configure the correct authentication and accounting port numbers.
    - When a controller is used as the RADIUS server, run the **netstat -nao** | **findstr 1812** and **netstat -nao** | **findstr 1813** commands on the server to check whether the ports are occupied. If yes, disable the applications that occupy the ports.
    - Check whether the IP address of the access control device is correct. If not, carry out the corresponding configuration to rectify this.

- The **test-aaa** command returns an account test failure.

  RADIUS authentication test for a single user fails.
  ```
  <Huawei> test-aaa user1 huawei123 radius-template huawei
  Info: Account test failed.
  ```

  RADIUS accounting test for a single user fails.
  ```
  <Huawei> test-aaa user1 huawei123 radius-template huawei accounting
  Info: Account test failed.
  ```

  - The possible causes are as follows:
    - The shared key of the RADIUS server is not configured.
    - The IP address of the RADIUS server is not configured.
  - Handling procedure:

 Copyright © Huawei Technologies Co., Ltd. 

        - Run the **display radius-server configuration** [ **template** *template-name* ] command in any view to check whether the shared key and IP address are configured in the RADIUS server template. If they are not the same, reconfigure the shared key and IP address in the RADIUS server template.
- After the **test-aaa** command is run, the test is passed, but authentication or accounting cannot be performed for the user.
  - The possible causes are as follows:
    - The route between the device and the server is unreachable.
    - The user authentication or accounting domain is different from the RADIUS authentication or accounting domain configured on the device.
  - Handling procedure:
    - Run the **ping** command to check whether a reachable route exists between the user and device. If there is no reachable route, establish a static route or use a routing protocol to establish a dynamic route between the device and the server.
    - Run the **display this** command in the AAA view to check whether the user authentication or accounting domain is the same as the RADIUS authentication or accounting domain configured on the device.
      - When the user name entered by the user contains a domain name, check whether RADIUS authentication or accounting has been configured in the domain. If not, configure RADIUS authentication or accounting in the domain.
      - When the user name entered by the user does not contain a domain name, check whether RADIUS authentication or accounting has been configured in the global default domain (administrator uses **default_admin** and common users use **default**). If not, configure RADIUS authentication or accounting in the domain.
    - Run the **display this** command in the AAA view to check whether the AAA authentication or accounting scheme and RADIUS server template have been applied to the domain. If not, apply the AAA authentication or accounting scheme and RADIUS server template to the domain.
    - If NAC has been configured, check whether the NAC configuration is correct. If not, correctly configure the NAC.

## 1.8.3 Configuring the AAA Alarm Report Function

### Context

You can configure the alarm report function, which helps you obtain real-time running status of AAA (for example, the status of the communication with the RADIUS server becomes Down) and facilitates O&M.

 Copyright © Huawei Technologies Co., Ltd. 

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **snmp-agent trap enable feature-name radius** [ **trap-name** { **hwradiusacctserverdown** | **hwradiusacctserverup** | **hwradiusauthserverdown** | **hwradiusauthserverup** } ]

The alarm report function is enabled for the RDS module.

By default, the alarm report function is disabled for the RDS module.

**----End**

### Verifying the Configuration

Run the **display snmp-agent trap feature-name radius all** command to view alarm status of the RDS module.

## 1.8.4 Recording Login and Logout Information

### Context

Enabling the recording of information related to normal logout, abnormal logout, and login failure helps administrators locate and analyze problems.

### Procedure

- Run the **aaa offline-record** command in the system view to record normal logout information.

  By default, the device is enabled to record normal logout information.
- Run the **aaa abnormal-offline-record** command in the system view to record abnormal logout information.

  By default, the device is enabled to record abnormal logout information.
- Run the **aaa online-fail-record** command in the system view to record login failure information.

  By default, the device is enabled to record login failure information.

**----End**

### Follow-up Procedure

- Run the **display aaa** { **offline-record** | **abnormal-offline-record** | **online-fail-record** } { **all** | **reverse-order** | **domain** *domain-name* | **interface** *interface-type interface-number* [ **vlan** *vlan-id* [ **qinq** *qinq-vlan-id* ] ] | **ip-address** *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **mac-address** *mac-address* | **access-slot** *slot-number* | **time** *start-time end-time* [ **date** *start-date end-date* ] | **username** *user-name* [ **time** *start-time end-time* [ **date** *start-date end-date* ] ] } [ **brief** ] to check normal logout, abnormal logout, and login failure records.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **display aaa statistics offline-reason** command in any view to check the reasons for users to go offline.

## 1.8.5 Clearing AAA Statistics

### Context

**NOTICE**

The AAA statistics cannot be restored after being cleared. Clear AAA statistics with caution.

Run the following commands to clear the statistics.

### Procedure

- Run the **reset aaa** { **abnormal-offline-record** | **offline-record** | **online-fail-record** } command in the system view to clear records of abnormal logout, logout, and login failures.
- Run the **reset aaa statistics offline-reason** command in any view to clear the statistics on reasons why users go offline.
- Run the **reset access-user statistics** command in any view to clear the statistics on access user authentication.
- Run the **reset hwtacacs-server statistics** { **accounting** | **all** | **authentication** | **authorization** } command in the user view to clear the statistics on HWTACACS authentication, accounting, and authorization.
- Run the **reset hwtacacs-server accounting-stop-packet** { **all** | **ip** { *ipv4-address* | *ipv6-address* } } command to clear remaining buffer information on HWTACACS accounting-stop packets.
- Run the **reset radius-server accounting-stop-packet** { **all** | **ip** { *ipv4-address* | *ipv6-address* } } command to clear remaining buffer information on RADIUS accounting-stop packets.
- Run the **reset local-user** [ *user-name* ] **password history record** command in the AAA view to clear historical passwords of local users.
- Run the **reset aaa statistics access-type-authenreq** command in any view to clear the number of authentication requests.

**----End**

## 1.8.6 Clearing HACA Statistics

### Context

Before collecting statistics within a certain period for fault locating, clear existing statistics.

 Copyright © Huawei Technologies Co., Ltd. 

NOTICE

The HACA statistics cannot be restored after being cleared. Confirm your operation before clearing the HACA statistics.

### Procedure

- Run the **reset haca-server statistics** { **all** | **message** | **packet** [ **register** | **accounting** | **authentication** | **authorization** | **user-syn** | **cut-notify** | **cut-request** ] } [ **template** *template-name* ] command in the user view to clear HACA statistics.
- Run the **reset haca-server accounting-stop-packet all** command in the user view to clear the remaining buffer information of HACA accounting-stop packets.

**----End**

# 1.9 Configuration Examples for AAA

## 1.9.1 Example for Configuring RADIUS Authentication and Accounting

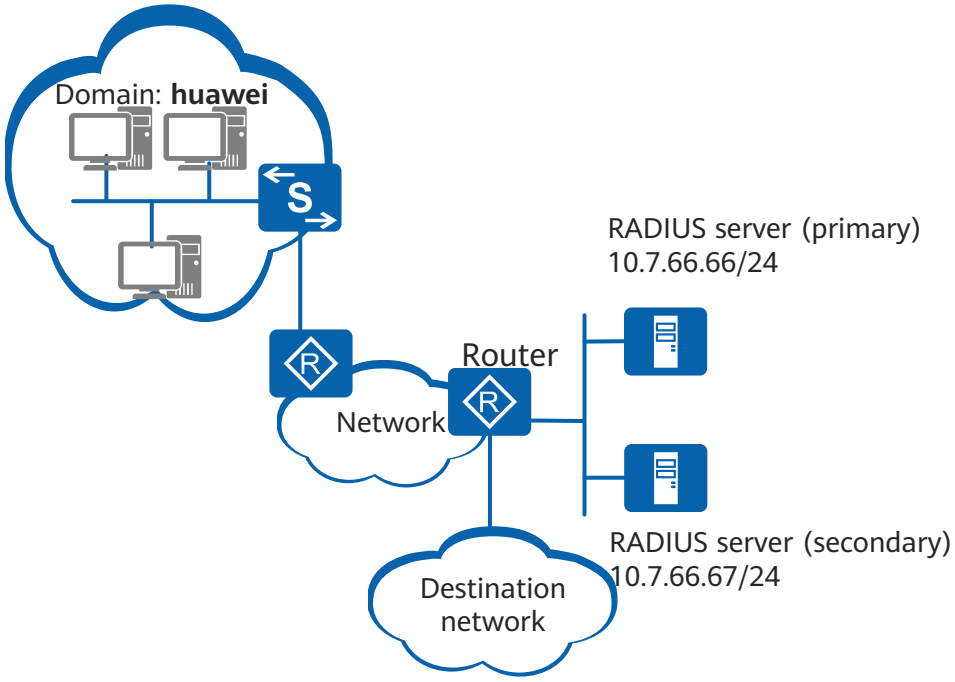
### Networking Requirements

As shown in **Figure 1-29**, users belong to the domain **huawei**. Router functions as the network access server on the destination network, providing access to users only after they are remotely authenticated by the server. The remote authentication on Router is described as follows:

- The RADIUS server will authenticate access users for Router. If RADIUS authentication fails, local authentication is used.
- The RADIUS servers at 10.7.66.66/24 and 10.7.66.67/24 function as the primary and secondary authentication and accounting servers, respectively. The default authentication port and accounting port are 1812 and 1813, respectively.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 1-29** Networking diagram of RADIUS authentication and accounting




## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a RADIUS server template.
2. Configure an authentication scheme and an accounting scheme.
3. Apply the RADIUS server template, authentication scheme, and accounting scheme to a domain.

NOTE

- Ensure that the devices are routable before the configuration.
- Ensure that the shared key in the RADIUS server template is the same as the setting on the RADIUS server.
- If the RADIUS server does not accept the user name containing the domain name, run the **undo radius-server user-name domain-included** command in the RADIUS server template view to configure the device to send packets that do not contain the domain name to the RADIUS server.
- After the domain is set to the global default domain, and the user name of a user carries the domain name or does not carry any domain name, the user uses AAA configuration information in the global default domain.
- After the **undo radius-server user-name domain-included** command is run, the device changes only the user name format in the sent packet, and the domain to which the user belongs is not affected. For example, after this command is run, the user with the user name **user@huawei.com** still uses AAA configuration information in the domain named **huawei.com**.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Configure a RADIUS server template.

# Configure a RADIUS template named **shiva**.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] radius-server template shiva
```

# Set the IP address and port numbers for the primary RADIUS authentication and accounting server.

```
[Router-radius-shiva] radius-server authentication 10.7.66.66 1812 weight 80
[Router-radius-shiva] radius-server accounting 10.7.66.66 1813 weight 80
```

# Set the IP address and port numbers for the secondary RADIUS authentication and accounting server.

```
[Router-radius-shiva] radius-server authentication 10.7.66.67 1812 weight 40
[Router-radius-shiva] radius-server accounting 10.7.66.67 1813 weight 40
```

# Set the shared key and retransmission count for the RADIUS server, and configure the device not to encapsulate the domain name in the user name when sending RADIUS packets to the RADIUS server.

```
[Router-radius-shiva] radius-server shared-key cipher Huawei@2012
[Router-radius-shiva] radius-server retransmit 2
[Router-radius-shiva] undo radius-server user-name domain-included
[Router-radius-shiva] quit
```

**Step 2** Configure authentication and accounting schemes.

# Create an authentication scheme named **auth**. Configure the authentication scheme to use RADIUS authentication as the active authentication mode and local authentication as the backup.

```
[Router] aaa
[Router-aaa] authentication-scheme auth
[Router-aaa-authen-auth] authentication-mode radius local
[Router-aaa-authen-auth] quit
```

# Create an accounting scheme named **abc**, and configure the accounting scheme to use the RADIUS accounting mode. Configure a policy for the device to keep users online upon accounting-start failures.

```
[Router-aaa] accounting-scheme abc
[Router-aaa-accounting-abc] accounting-mode radius
[Router-aaa-accounting-abc] accounting start-fail online
[Router-aaa-accounting-abc] quit
```

**Step 3** Create a domain named **huawei**, and apply the authentication scheme **auth**, accounting scheme **abc**, and RADIUS server template **shiva** to the domain.

```
[Router-aaa] domain huawei
[Router-aaa-domain-huawei] authentication-scheme auth
[Router-aaa-domain-huawei] accounting-scheme abc
[Router-aaa-domain-huawei] radius-server shiva
[Router-aaa-domain-huawei] quit
[Router-aaa] quit
```

**Step 4** Set the domain **huawei** to the global default domain.

```
[Router] domain huawei
[Router] domain huawei admin
```

**Step 5** Configure local authentication.

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router] aaa
[Router-aaa] local-user user1 password irreversible-cipher Huawei@123
[Router-aaa] local-user user1 service-type http
[Router-aaa] local-user user1 privilege level 15
[Router-aaa] quit
```

**Step 6** Verify the configuration.

# Run the **display radius-server configuration template** *template-name* command on Router to verify the RADIUS server template configuration.

```
[Router] display radius-server configuration template shiva
 ------------------------------------------------------------------------------
 Server-template-name         : shiva
 Protocol-version             : standard
 Traffic-unit                 : B
 Shared-secret-key            : %^%#z3#CA>MtbD=>A]Ts;au$;&I!<sN~"B!++2S8'--;%^%#
 Group-filter                 : class
 Timeout-interval(in second)  : 5
 Retransmission               : 2
 EndPacketSendTime            : 3
 Dead time(in minute)         : 5
 Domain-included              : NO
 NAS-IP-Address               : -
 Calling-station-id MAC-format : xxxx-xxxx-xxxx
 Called-station-id MAC-format  : XX-XX-XX-XX-XX-XX
 NAS-Port-ID format           : New
 Service-type                 : -
 NAS-IPv6-Address             : ::
 Server algorithm             : master-backup
 Detect-interval(in second)   : 60
 Authentication Server 1      : 10.7.66.66     Port:1812  Weight:80  [UP]
                                Vrf:- LoopBack:NULL Vlanif:NULL
                                Source IP: ::
 Authentication Server 2      : 10.7.66.67     Port:1812  Weight:40  [UP]
                                Vrf:- LoopBack:NULL Vlanif:NULL
                                Source IP: ::
 Accounting Server    1       : 10.7.66.66     Port:1813  Weight:80  [UP]
                                Vrf:- LoopBack:NULL Vlanif:NULL
                                Source IP: ::
 Accounting Server    2       : 10.7.66.67     Port:1813  Weight:40  [UP]
                                Vrf:- LoopBack:NULL Vlanif:NULL
                                Source IP: ::
 ------------------------------------------------------------------------------
```

**----End**

## Configuration Files

Router configuration file

```
#
 sysname Router
#
domain huawei
domain huawei admin
#
radius-server template shiva
 radius-server shared-key cipher %^%#z3#CA>MtbD=>A]Ts;au$;&I!<sN~"B!++2S8'--;%^%#
 radius-server authentication 10.7.66.66 1812 weight 80
 radius-server authentication 10.7.66.67 1812 weight 40
 radius-server accounting 10.7.66.66 1813 weight 80
 radius-server accounting 10.7.66.67 1813 weight 40
 radius-server retransmit 2
 undo radius-server user-name domain-included
#
aaa
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 authentication-scheme auth
  authentication-mode radius local
 accounting-scheme abc
  accounting-mode radius
  accounting start-fail online
 domain huawei
  authentication-scheme auth
  accounting-scheme abc
  radius-server shiva
 local-user user1 password irreversible-cipher
 local-user user1 privilege level 15
 local-user user1 service-type http
#
return
```

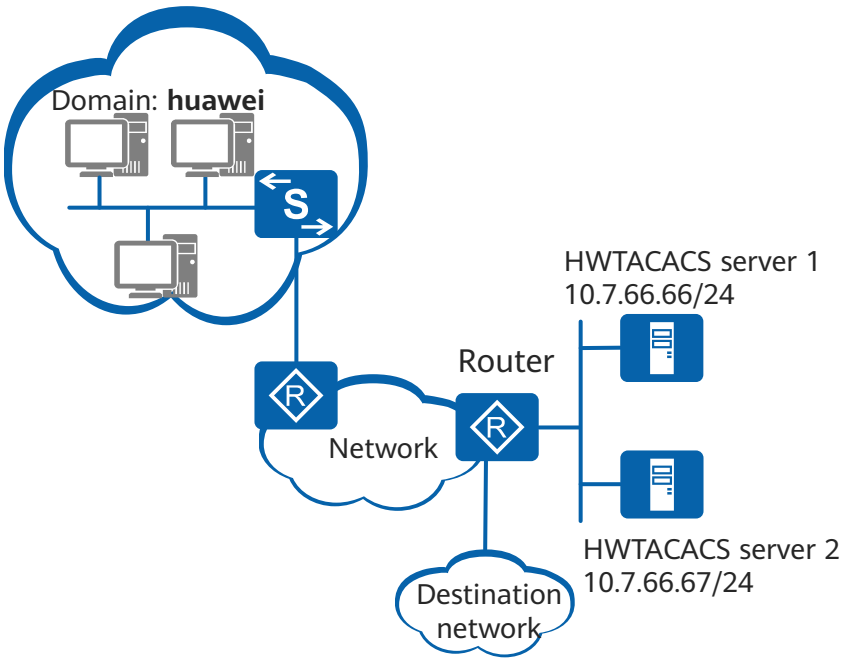
# 1.9.2 Example for Configuring HWTACACS Authentication, Accounting, and Authorization

## Networking Requirements

For the network shown in **Figure 1-30**, the customer requirements are as follows:

- The HWTACACS server will authenticate access users for Router. If HWTACACS authentication fails, local authentication is used.
- The HWTACACS server will authorize access users for Router. If HWTACACS authorization fails, local authorization is used.
- HWTACACS accounting is used by Router for access users.
- Real-time accounting is performed every 3 minutes.
- The IP addresses of primary and secondary HWTACACS servers are 10.7.66.66/24 and 10.7.66.67/24, respectively. The port number for authentication, accounting, and authorization is 49.

**Figure 1-30** Networking diagram of HWTACACS authentication, accounting, and authorization




 Copyright © Huawei Technologies Co., Ltd. 

## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an HWTACACS server template.
2. Configure authentication, authorization, and accounting schemes.
3. Apply the HWTACACS server template, authentication scheme, authorization scheme, and accounting scheme to a domain.

NOTE

- Ensure that the devices are routable before the configuration.
- Ensure that the shared key in the HWTACACS server template is the same as the settings on the HWTACACS server.
- If the HWTACACS server does not accept the user name containing the domain name, run the **undo hwtacacs-server user-name domain-included** command in the HWTACACS server template view to configure the device to send packets that do not contain the domain name to the HWTACACS server.
- After the domain is set to the global default domain, and the user name of a user carries the domain name or does not carry any domain name, the user uses AAA configuration information in the global default domain.
- After the **undo hwtacacs-server user-name domain-included** command is run, the device changes only the user name format in the sent packet, and the domain to which the user belongs is not affected. For example, after this command is run, the user with the user name **user@huawei.com** still uses AAA configuration information in the domain named **huawei.com**.

## Procedure

**Step 1** Enable HWTACACS.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] hwtacacs enable
```

NOTE

By default, HWTACACS is enabled. If the HWTACACS settings are not modified, you can skip this step.

**Step 2** Configure an HWTACACS server template.

# Create an HWTACACS server template named **ht**.

```
[Router] hwtacacs-server template ht
```

# Set the IP addresses and port numbers for the primary HWTACACS authentication, authorization, and accounting servers.

```
[Router-hwtacacs-ht]  hwtacacs-server authentication 10.7.66.66 49
[Router-hwtacacs-ht] hwtacacs-server authorization 10.7.66.66 49
[Router-hwtacacs-ht] hwtacacs-server accounting 10.7.66.66 49
```

# Set the IP addresses and port numbers for the secondary HWTACACS authentication, authorization, and accounting servers.

```
[Router-hwtacacs-ht] hwtacacs-server authentication 10.7.66.67 49 secondary
[Router-hwtacacs-ht] hwtacacs-server authorization 10.7.66.67 49 secondary
[Router-hwtacacs-ht] hwtacacs-server accounting 10.7.66.67 49 secondary
```

 Copyright © Huawei Technologies Co., Ltd. 

# Set the shared key for the HWTACACS server.

NOTE

Ensure that the shared key in the HWTACACS server template is the same as that set on the HWTACACS server.

```
[Router-hwtacacs-ht] hwtacacs-server shared-key cipher Huawei@2012
[Router-hwtacacs-ht] quit
```

**Step 3** Configure authentication, authorization, and accounting schemes.

# Create an authentication scheme named **l-h**. Configure the authentication scheme to use HWTACACS authentication as the active authentication mode and local authentication as the backup.

```
[Router] aaa
[Router-aaa] authentication-scheme l-h
[Router-aaa-authen-l-h] authentication-mode hwtacacs local
[Router-aaa-authen-l-h] quit
```

# Create an authorization scheme named **hwtacacs**. Configure the authorization scheme to use HWTACACS authorization as the active authorization mode and local authorization as the backup.

```
[Router-aaa] authorization-scheme hwtacacs
[Router-aaa-author-hwtacacs] authorization-mode hwtacacs local
[Router-aaa-author-hwtacacs] quit
```

# Create an accounting scheme named **hwtacacs**, and configure the accounting scheme to use the HWTACACS accounting mode. Configure a policy for the device to keep users online upon accounting-start failures.

```
[Router-aaa] accounting-scheme hwtacacs
[Router-aaa-accounting-hwtacacs] accounting-mode hwtacacs
[Router-aaa-accounting-hwtacacs] accounting start-fail online
```

# Set the real-time accounting interval to 3 minutes.

```
[Router-aaa-accounting-hwtacacs] accounting realtime 3
[Router-aaa-accounting-hwtacacs] quit
```

**Step 4** Create a domain named **huawei**, and apply the authentication scheme **l-h**, authorization scheme **hwtacacs**, accounting scheme **hwtacacs**, and the HWTACACS server template **ht** to the domain.

```
[Router-aaa] domain huawei
[Router-aaa-domain-huawei] authentication-scheme l-h
[Router-aaa-domain-huawei] authorization-scheme hwtacacs
[Router-aaa-domain-huawei] accounting-scheme hwtacacs
[Router-aaa-domain-huawei] hwtacacs-server ht
[Router-aaa-domain-huawei] quit
[Router-aaa] quit
```

**Step 5** Configure local authentication.

```
[Router] aaa
[Router-aaa] local-user user1 password irreversible-cipher Huawei@123
[Router-aaa] local-user user1 service-type http
[Router-aaa] local-user user1 privilege level 15
[Router-aaa] quit
```

**Step 6** Configure the global default domain for administrations.

```
[Router] domain huawei admin
```

**Step 7** Verify the configuration.

 Copyright © Huawei Technologies Co., Ltd. 

# Run the **display hwtacacs-server template** command on Router to verify the HWTACACS server template configuration.

```
[Router] display hwtacacs-server template ht
  ------------------------------------------------------------------------------
  HWTACACS-server template name   : ht
  Primary-authentication-server   : 10.7.66.66:49:-
  Primary-authorization-server    : 10.7.66.66:49:-
  Primary-accounting-server       : 10.7.66.66:49:-
  Secondary-authentication-server : 10.7.66.67:49:-
  Secondary-authorization-server  : 10.7.66.67:49:-
  Secondary-accounting-server     : 10.7.66.67:49:-
  Third-authentication-server     : -:0:-
  Third-authorization-server      : -:0:-
  Third-accounting-server         : -:0:-
  Current-authentication-server   : 10.7.66.66:49:-
  Current-authorization-server    : 10.7.66.66:49:-
  Current-accounting-server       : 10.7.66.66:49:-
  Source-IP-address               : -
  Source-IPv6-address             : ::
  Shared-key                      : **********
  Quiet-interval(min)             : 5
  Response-timeout-Interval(sec)  : 5
  Domain-included                 : Original
  Traffic-unit                    : B
  ------------------------------------------------------------------------------
```

# Run the **display domain** command on Router to verify the domain configuration.

```
[Router] display domain name huawei
  Domain-name                     : huawei
  Domain-index                    : 2
  Domain-state                    : Active
  Authentication-scheme-name      : l-h
  Accounting-scheme-name          : hwtacacs
  Authorization-scheme-name       : hwtacacs
  Service-scheme-name             : -
  RADIUS-server-template          : default
  HWTACACS-server-template        : ht
  User-group                      : -
  Push-url-address                : -
  Flow-statistic                  : -
  Tariff-level                    : -
```

**----End**

## Configuration Files

Router configuration file

```
#
 sysname Router
#
domain huawei admin
#
hwtacacs-server template ht
 hwtacacs-server authentication 10.7.66.66
 hwtacacs-server authentication 10.7.66.67 secondary
 hwtacacs-server authorization 10.7.66.66
 hwtacacs-server authorization 10.7.66.67 secondary
 hwtacacs-server accounting 10.7.66.66
 hwtacacs-server accounting 10.7.66.67 secondary
 hwtacacs-server shared-key cipher %^%#0%i9M.C!T$8iTn7Ig-4V8GTgK[gwp3b6;k=caxl-%^%#
#
aaa
 authentication-scheme l-h
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 authentication-mode hwtacacs local
 authorization-scheme hwtacacs
  authorization-mode hwtacacs local
 accounting-scheme hwtacacs
  accounting-mode hwtacacs
  accounting realtime 3
  accounting start-fail online
 domain huawei
  authentication-scheme l-h
  accounting-scheme hwtacacs
  authorization-scheme hwtacacs
  hwtacacs-server ht
 local-user user1 password irreversible-cipher $1a$8&/1M*R6{A$#D_UJt7Vv1L5LI*A_l=UdI)WLj|dhD~oxy=
$O[}F$
 local-user user1 privilege level 15
 local-user user1 service-type http
#
return
```

# 1.9.3 Example for Configuring Domain-based User Management

## Networking Requirements

As shown in **Figure 1-31**, enterprise users access the network through Router. The user names do not contain any domain names.

The enterprise requires that common users access the network and obtain rights after passing RADIUS authentication and that administrators log in to the device for management only after passing local authentication on Router.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 1-31** Configuring domain-based user management

## Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN and a VLANIF interface for Router to communicate with the RADIUS server.
2. Configure authentication and accounting schemes for common users and apply the schemes to the **default** domain to authenticate common users, such as users using 802.1X authentication. The user names of the users do not contain domain names.
3. Configure authentication and authorization schemes for administrators and apply the schemes to the **default_admin** domain to authenticate administrators, such as a user logging in through Telnet, SSH, or FTP. The user names of administrators do not contain domain names.

NOTE

Ensure that users have been configured on the RADIUS server. In this example, the user with the user name **test1** and password **123456** has been configured on the RADIUS server.

This example provides only the configuration for Router. The configurations of the RADIUS server are not described here.

## Procedure

**Step 1** Create a VLAN and configure interfaces.

# Create VLAN 11 on Router.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 11
```

# Set the link type of Eth2/0/1 of Router that is connected to the RADIUS server to **access**, and add Eth2/0/1 to VLAN 11.

```
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type access
[Router-Ethernet2/0/1] port default vlan 11
[Router-Ethernet2/0/1] quit
```

# Create VLANIF 11, and configure the IP address of 192.168.2.29/24 for VLANIF 11.

```
[Router] interface vlanif 11
[Router-Vlanif11] ip address 192.168.2.29 24
[Router-Vlanif11] quit
```

**Step 2** Configure RADIUS AAA for common users who use 802.1X authentication.

NOTE

Ensure that the shared key in the RADIUS server template is the same as that set on the RADIUS server.

# Configure a RADIUS server template named **rd1**.

```
[Router] radius-server template rd1
[Router-radius-rd1] radius-server authentication 192.168.2.30 1812
[Router-radius-rd1] radius-server accounting 192.168.2.30 1813
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router-radius-rd1] radius-server shared-key cipher Huawei@2012
[Router-radius-rd1] radius-server retransmit 2
[Router-radius-rd1] quit
```

# Create authentication and accounting schemes both named **abc**, and set the authentication and accounting modes to RADIUS.

```
[Router] aaa
[Router-aaa] authentication-scheme abc
[Router-aaa-authen-abc] authentication-mode radius
[Router-aaa-authen-abc] quit
[Router-aaa] accounting-scheme abc
[Router-aaa-accounting-abc] accounting-mode radius
[Router-aaa-accounting-abc] quit
```

# Test connectivity between Router and the RADIUS server. Ensure that the **test1** user with the password **123456** has been configured on the RADIUS server.

```
[Router-aaa] test-aaa test1 123456 radius-template rd1
```

# Apply the authentication scheme **abc**, accounting schemes **abc**, and RADIUS server template **rd1** to the **default** domain.

```
[Router-aaa] domain default
[Router-aaa-domain-default] authentication-scheme abc
[Router-aaa-domain-default] accounting-scheme abc
[Router-aaa-domain-default] radius-server rd1
[Router-aaa-domain-default] quit
[Router-aaa] quit
```

# Enable 802.1X authentication on GE2/0/0.

```
[Router] dot1x-access-profile name d1
[Router-dot1x-access-profile-d1] quit
[Router] authentication-profile name p1
[Router-authen-profile-p1] dot1x-access-profile d1
[Router-authen-profile-p1] authentication mode multi-authen max-user 100
[Router-authen-profile-p1] quit
[Router] vlan batch 10
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type access
[Router-Ethernet2/0/0] port default vlan 10
[Router-Ethernet2/0/0] authentication-profile p1
[Router-Ethernet2/0/0] quit
```

# Set the global default domain for common users to **default**. After common users enter their user names in the format of *user***@default**, the device performs AAA authentication for the users in the **default** domain. If a user name does not contain a domain name or contains a non-existing domain name, the device authenticates the common user in the default domain for common users.

```
[Router] domain default
```

**Step 3** Configure local authentication and authorization for the administrator **test**.

# Configure the device to use AAA for the Telnet user that logs in through the VTY user interface.

```
[Router] telnet server enable
[Router] user-interface vty 0 14
[Router-ui-vty0-14] authentication-mode aaa
[Router-ui-vty0-14] quit
```

# Configure a local user named **test** with password **admin@12345**, and set the user level to 3.

```
[Router] aaa
[Router-aaa] local-user test password irreversible-cipher admin@12345 privilege level 3
```

 Copyright © Huawei Technologies Co., Ltd. 

# Set the access type of **test** to Telnet.

```
[Router-aaa] local-user test service-type telnet
```

# Configure local account locking. Set the retry interval to 5 minutes, the maximum number of consecutive authentication failures to 3, and the local account locking duration to 5 minutes.

```
[Router-aaa] local-aaa-user wrong-password retry-interval 5 retry-time 3 block-time 5
```

# Create an authentication scheme named **auth**, and configure the authentication scheme to use local authentication.

```
[Router-aaa] authentication-scheme auth
[Router-aaa-authen-auth] authentication-mode local
[Router-aaa-authen-auth] quit
```

# Create an authorization scheme named **autho**, and configure the authorization scheme to use local authorization.

```
[Router-aaa] authorization-scheme autho
[Router-aaa-author-autho] authorization-mode local
[Router-aaa-author-autho] quit
```

# Apply the authentication scheme **auth** and authorization scheme **autho** to the **default_admin** domain.

```
[Router-aaa] domain default_admin
[Router-aaa-domain-default_admin] authentication-scheme auth
[Router-aaa-domain-default_admin] authorization-scheme autho
[Router-aaa-domain-default_admin] quit
[Router-aaa] quit
```

# Set the global default domain for administrators to **default_admin**. After administrators enter user names in the format of *user*@**default_admin**, the device performs AAA authentication for the administrators in the **default_admin** domain. If the user name of an administrator does not contain a domain name or contains a non-existing domain name, the device authenticates the administrator in the default domain for administrators.

```
[Router] domain default_admin admin
[Router] quit
```

**Step 4** Verify the configuration.

# Run the **display dot1x interface** command on Router to verify the 802.1X authentication configuration.

# If you log in as a common user, enter the user name **test1** and password **123456** on an 802.1X client, and run the **display access-user domain** and **display access-user user-id** commands to check the domain to which you belong and your access type.

```
<Router> display access-user domain default
--------------------------------------------------------------------------------
UserID Username          IP address          MAC              Status
--------------------------------------------------------------------------------
16040  test1             -                   00e0-4c97-31f6   Success
--------------------------------------------------------------------------------
Total: 1, printed: 1
<Router> display access-user user-id 16040
Basic:
  User id                     : 16040
  User name                   : test1
  Domain-name                 : default
```

 Copyright © Huawei Technologies Co., Ltd. 

```
  User MAC                     : 00e0-4c97-31f6
  User IP address              : -
  User IPv6 address            : -
  User access time             : 2009/02/15 19:10:52
  User accounting session ID   : huawei255255000000000f****2016040
  Option82 information         : -
  User access type             : 802.1x

AAA:
  User authentication type     : 802.1x authentication
  Current authentication method  : RADIUS
  Current authorization method   : -
  Current accounting method      : RADIUS
```

# If you log in through Telnet, enter the user name **test** and password **admin@12345**, and run the **display access-user domain** and **display access-user user-id** commands to check the domain to which you belong and your access type.

```
<Router> display access-user domain default_admin
 ------------------------------------------------------------------------------
 UserID Username          IP address          MAC              Status
 ------------------------------------------------------------------------------
 16009  test              10.135.18.217       -                Success
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
<Router> display access-user user-id 16009
Basic:
  User id                    : 16009
  User name                  : test
  Domain-name                : default_admin
  User MAC                   : -
  User IP address            : 10.135.18.217
  User IPv6 address          : -
  User access time           : 2009/02/15 05:10:52
  User accounting session ID   : huawei255255000000000f****2016009
  Option82 information         : -
  User access type           : Telnet

AAA:
  User authentication type     : Administrator authentication
  Current authentication method  : Local
  Current authorization method   : Local
  Current accounting method      : None
```

**----End**

## Configuration File

Router configuration file

```
#
sysname Router
#
vlan batch 10 to 11
#
authentication-profile name p1
 dot1x-access-profile d1
 authentication mode multi-authen max-user 100
#
radius-server template rd1
 radius-server shared-key cipher %^%#Q75cNQ6IF(e#L4WMxP~%^7'u17,]D87GO{"[o]`D%^%#
 radius-server authentication 192.168.2.30 1812 weight 80
 radius-server accounting 192.168.2.30 1813 weight 80
 radius-server retransmit 2
#
aaa
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 authentication-scheme abc
  authentication-mode radius
 authentication-scheme auth
 authorization-scheme autho
 accounting-scheme abc
  accounting-mode radius
 domain default
  authentication-scheme abc
  accounting-scheme abc
  radius-server rd1
 domain default_admin
  authentication-scheme auth
  authorization-scheme autho
 local-user test password irreversible-cipher $1a$KQje%Ip2q/$bBk."}ISO@KQje%Ip2q/$bBk."}ISO@$
 local-user test privilege level 3
 local-user test service-type telnet
#
interface Vlanif11
 ip address 192.168.2.29 255.255.255.0
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 10
 authentication-profile p1
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 11
#
 telnet server enable
#
user-interface vty 0 14
 authentication-mode aaa
#
dot1x-access-profile name d1
#
return
```

# 1.10 FAQ About AAA

## 1.10.1 Why Must the Administrator Pass the AAA Authentication?

To ensure device security, the administrator must be authenticated by AAA authentication in local or remote authentication mode. The administrator, however, can log in to the device in non-authentication mode in the VTY interface view.

## 1.10.2 Why Does RADIUS Authentication Fail When the RADIUS Server Template and RADIUS Server Are Properly Configured?

This problem has the following possible causes:

- The IP address of the router (a RADIUS client) is not configured on the RADIUS server, so the RADIUS server cannot send an authentication response packet to the router.
- Different shared keys are configured on the router and the RADIUS server.

 Copyright © Huawei Technologies Co., Ltd. 

## 1.10.3 Why Does the Server Checking Error Occur During RADIUS Dynamic Authentication?

This error occurs because the RADIUS authentication server is not configured properly.

## 1.10.4 Why Does HWTACACS Authentication Fail When the HWTACACS Server Template and HWTACACS Server Are Properly Configured?

This failure has the following possible causes:

- The IP address of the router (a client) is not configured on the HWTACACS server, so the HWTACACS server cannot send an authentication response packet to the router .
- Different shared keys are configured on the router and the HWTACACS server.

## 1.10.5 Why Are Accounting Packets Received When Commands Are Run on Devices?

This occurs so that devices can record history commands. To disable this function, run the **undo cmd recording-scheme** command in the AAA view.

## 1.10.6 Why Are the 802.1x Users' IP Addresses Not Displayed After I Run the Display Access-User Command?

The device learns the IP address of an authenticated online user from ARP packets that the user sends. If the user does not send any ARP packets, the device cannot learn or display the user's IP address.

## 1.10.7 Which Attributes Are Required by ACLs Dynamically Delivered by the RADIUS Server?

| No. | Type | Value | Standard Attribute | Description |
| --- | --- | --- | --- | --- |
| 31 | string | User MAC address. | Yes | - |
| 11 | string | ACL number | Yes | You can select either of the two attributes. |
| 82 | string | ACL description | No. It is a private attribute designed by Huawei. | |

 Copyright © Huawei Technologies Co., Ltd. 

## 1.10.8 Which Attributes Are Required by VLANs Dynamically Delivered by the RADIUS Server?

| No. | Type | Value | Standard Attribute |
| --- | --- | --- | --- |
| 31 | string | User MAC address. | Yes |
| 64 | integer | 13 | Yes |
| 65 | integer | 6 | Yes |
| 81 | string | VLAN ID | Yes |

## 1.10.9 What Are the Restrictions on Using HWTACACS?

The HWTACACS template used by users, bound to domains, or referenced by accounting stop packets cannot be deleted.

If the HWTACACS server is sending packets, the server IP address cannot be changed.

## 1.10.10 Does the Router Support User Level Settings Using RADIUS? How Can I Configure It?

Yes, the router can set user levels using RADIUS. The configuration effect is the same as the local user level configuration during AAA local authentication.

You can set the user levels on the RADIUS server.

## 1.10.11 Level 1 Is Configured for a User on the RADIUS Server, But the User Has More Rights Than Rights Defined in Level 1 After Login. Why?

Run the **display current-configuration** command to check the device configuration and check whether the **command-privilege level** command is used to change the level.

## 1.10.12 How Do I Convert RADIUS Attributes After Replacing an ME60 Gateway with an AR Router?

After an AR router replaces an ME60 gateway, some RADIUS attributes of the AR router need to be converted into corresponding RADIUS attributes of the ME60 gateway so that the AR router can properly connect to the RADIUS server.

For example, the mapping of Huawei proprietary attributes of the AR router and ME60 gateway is as follows:

 Copyright © Huawei Technologies Co., Ltd. 

- Proprietary RADIUS attribute 1 (HW-Input-Peak-Information-Rate) of the AR router corresponds to proprietary RADIUS attribute 3 of the ME60 gateway.
- Proprietary RADIUS attribute 3 (HW-Input-Committed-Burst-Size) of the AR router corresponds to proprietary RADIUS attribute 1 of the ME60 gateway.

According to the preceding mapping, convert proprietary RADIUS attribute 1 to proprietary RADIUS attribute 3, and proprietary RADIUS attribute 3 to proprietary RADIUS attribute 1 on the AR router.

- Run the **radius-server attribute translate** command in the RADIUS server template view to enable RADIUS attribute translation.
- Run the **radius-attribute translate HW-Input-Peak-Information-Rate HW-Input-Committed-Burst-Size receive** command in the RADIUS server template view to convert proprietary RADIUS attribute 1 in received packets to proprietary RADIUS attribute 3.
- Run the **radius-attribute translate HW-Input-Committed-Burst-Size HW-Input-Peak-Information-Rate receive** command in the RADIUS server template view to convert proprietary RADIUS attribute 3 in received packets to proprietary RADIUS attribute 1.

When receiving packets containing proprietary RADIUS attribute 1 or 3 from the RADIUS server, the AR router can properly obtain attribute information.

For the mapping between other attributes, for example, between proprietary RADIUS attribute 4 (HW-Output-Peak-Information-Rate) of the AR router and proprietary RADIUS attribute 6 of the ME60 gateway, you can configure attribute translation similarly. For details about the mapping between attributes, see the RADIUS attribute table for the AR router and that for the ME60 gateway in the corresponding product documentation.

 Copyright © Huawei Technologies Co., Ltd. 

# 2 DAA Configuration

## About This Chapter

2.1 Overview of DAA
2.2 Understanding DAA
2.3 Application Scenarios for DAA
2.4 Summary of DAA Configuration Tasks
2.5 Licensing Requirements and Limitations for DAA
2.6 Default Settings for DAA
2.7 Configuring DAA
2.8 Configuration Examples for DAA

## 2.1 Overview of DAA

### Definition

Destination Address Accounting (DAA) technology implements accounting based on the destination addresses users access.

### Purpose

On a network where users need to pay for the network access service, the Internet service provider (ISP) does not charge the users when they access only internal network resources or charges these users a little money. However, the ISP charges the users a lot of money when they access external network resources.

DAA technology separates the campus network from the external network. To be specific, DAA differentiates services according to destination addresses and enforces different traffic statistics collection and accounting policies. Therefore, DAA helps ISPs implement delicacy operation and accounting based on service types.

 Copyright © Huawei Technologies Co., Ltd. 

# 2.2 Understanding DAA

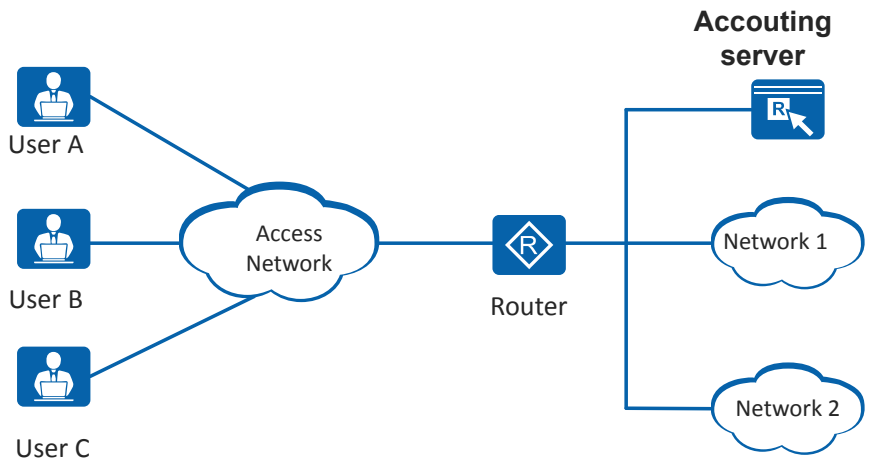
## Concepts

- Traffic identification: classifies traffic into different types according to the destination IP addresses users access.
- Tariff level: identifies the data flows destined for the specified address so that the device can collect statistics and enforce differentiated policies on different types of traffic.
- Traffic group: associates classified traffic with tariff levels.

## Implementation

Figure 2-1 shows the network of DAA service. The Router works with an accounting server to implement destination-based accounting.

**Figure 2-1** Network of DAA service




During a user authentication and network access process, DAA service process is as follows:

NOTE

This process assumes that users have passed authentication.

1. A user goes online and traffic is generated.
2. When the user accesses Network1 or Network2, the device resolves the destination address from user traffic, and matches the destination address against ACL, which is the traffic identification rule.

 Copyright © Huawei Technologies Co., Ltd. 

3. The device obtains the tariff level corresponding to the ACL in the traffic group, and maps the traffic to the corresponding tariff level.
4. The device performs traffic statistics collection according to the tariff level.
5. (Optional) The device periodically sends an interim accounting packet to the accounting server. The packet carries accumulative traffic statistics corresponding to each tariff level.
6. (Optional) After receiving an interim accounting packet, the accounting server parses traffic information corresponding to each tariff level and performs interim accounting based on certain rules.
7. When the user requests to go offline, the device sends an accounting stop packet to the accounting server. The packet carries traffic statistics at each tariff level during this online process of the user.
8. After receiving an accounting stop packet, the accounting server parses traffic information corresponding to each tariff level during the entire online process and performs accounting based on certain rules.
9. The user goes offline.

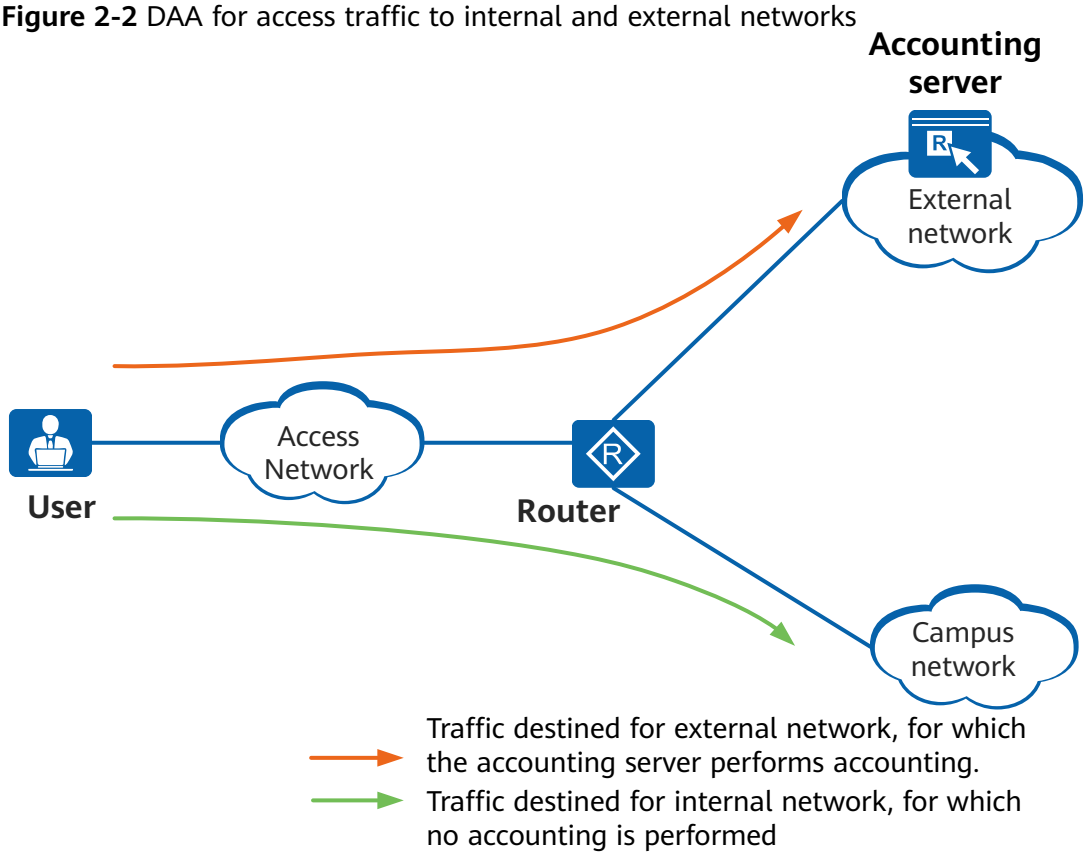
# 2.3 Application Scenarios for DAA

As shown in **Figure 2-2**, users on the campus network of a university can access resources on the campus network or external network through the Router. The campus network built by the university provides a large number of learning materials, which are free for internal users. The external network is leased from the ISP. The users need to be charged when they access the external network resources.

After DAA is configured, when users access external network resources, the device collects statistics on traffic and sends the statistics to the accounting server. The accounting server then performs accounting. When users access internal network resources, the device collects statistics on traffic but does not send the statistics to the accounting server. The accounting server does not perform accounting.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 2-2** DAA for access traffic to internal and external networks




# 2.4 Summary of DAA Configuration Tasks

Table 2-1 lists DAA configuration tasks.

**Table 2-1** DAA configuration tasks

| Scenario | Description | Task |
| --- | --- | --- |
| The device performs accounting for users when the users access specified destination addresses. | The administrator wants to charge the users who access the specified destination networks due to some reasons. You can configure traffic identification rules so that the device can identify the traffic going to the specified destination networks and collect statistics on the traffic. Then the device sends the collected statistics to the accounting server. The destination-based accounting is implemented. | 1. 2.7.1 Configuring Traffic Identification Rules<br>2. 2.7.2 Configuring the Tariff Level<br>3. 2.7.3 Configuring Traffic-based Accounting |


Copyright © Huawei Technologies Co., Ltd.

| Scenario | Description | Task |
| --- | --- | --- |
| The device performs accounting for users when the users access external networks. | On a network where users need to pay for the network access service, for example, a campus network, the Internet service provider (ISP) does not charge the users when they access the internal network resources, while charges the users when they access the external network resources.<br>The administrator knows all the internal network segments, but it is difficult to predict the external network segments the users want to access. Therefore, the device cannot accurately collect traffic statistics on the external network segments. To address this issue, you can configure the traffic identification rule that separates the traffic going to internal and external network segments. The device does not collect statistics on the internal network segments, and sends statistics on all the traffic, except the traffic going to internal network segments, to the accounting server. By using this method, the device performs accounting for users when they access external networks while does not perform accounting for users when they access internal networks. | 1. **2.7.1 Configuring Traffic Identification Rules**<br>2. **2.7.2 Configuring the Tariff Level**<br>3. **2.7.3 Configuring Traffic-based Accounting**<br>4. Run the **statistic enable (AAA domain view)** command in the AAA domain view to enable traffic statistics collection for domain users. The device then collects statistics on all the traffic except the traffic corresponding to the specified tariff level. |


Copyright © Huawei Technologies Co., Ltd.

# 2.5 Licensing Requirements and Limitations for DAA

## Involved Network Elements

**Table 2-2** Components involved in NAC networking

| Role | Product Model | Description |
| --- | --- | --- |
| AAA server | Huawei servers or third-party AAA servers | Performs authentication, accounting, and authorization on users. |
| Portal server | Huawei servers or third-party Portal servers | Receives authentication requests from Portal clients, provides free portal services and an interface based on web authentication, and exchanges authentication information of the authentication clients with access devices.<br>This component is required only in external Portal authentication mode. |

## Licensing Requirements

DAA is a basic feature of the device and is not under license control.

## Feature Limitations

None

# 2.6 Default Settings for DAA

Table 2-3 lists the default settings for DAA.

**Table 2-3** Default settings for DAA

| Parameter | Default Setting |
| --- | --- |
| Traffic identification rule | None |
| Tariff level | None |


Copyright © Huawei Technologies Co., Ltd.

| Parameter | Default Setting |
| --- | --- |
| Statistics collection on the traffic corresponding to the specified tariff level | Disabled |
| Accounting on the traffic corresponding to the specified tariff level | Disabled |

# 2.7 Configuring DAA

## Pre-configuration Tasks

DAA provides a destination-based accounting scheme, but the DAA function cannot implement the scheme alone. Before configuring DAA, complete the following tasks:

- Configure Portal, or PPPoE authentication.

  For details, see **3.6 Configuring NAC** or **PPPoE Configuration**.

  NOTE

  DAA supports only Portal or PPPoE authentication. If Portal authentication is used, you must configure Portal authentication on a routed main interface.

- Configure RADIUS authentication and accounting.

  For details, see **Configuring RADIUS Authentication, Authorization, and Accounting** in **AAA Configuration**.

# 2.7.1 Configuring Traffic Identification Rules

## Context

To implement destination-based accounting, the device must be able to identify the traffic destined for different networks according to access control lists (ACLs).

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Configure traffic identification rules.

1. Run **acl** [ **number** ] *acl-number* [ **match-order** { **auto** | **config** } ]

   An advanced ACL is created by using an ACL number and the advanced ACL view is displayed.

   Or run **acl name** *acl-name* { **advance** | *acl-number* } [ **match-order** { **auto** | **config** } ]

   An advanced ACL is created by using an ACL name and the advanced ACL view is displayed.


Copyright © Huawei Technologies Co., Ltd.

By default, no ACL exists on the device.

2. Run **rule** [ *rule-id* ] **permit ip** { **source** { *source-ip-address* { *source-wildcard* | *src-netmask* } | **any** } | **destination** { *destination-ip-address* { *destination-wildcard* | *des-netmask* } | **any** } } *

An advanced ACL rule is created.

By default, no ACL rule exists on the device.

NOTE

The number of an advanced ACL is in the range from 3000 to 3999.

The ACL (with the number in the range of 3000-3031) configured or modified for wireless users takes effect only after being delivered to APs by the **commit** command.

The destination address is mandatory and the source address is optional. You can configure both the source and destination addresses to precisely specify the traffic on which accounting is performed.

If the **any** parameter is configured to specify all source and destination addresses, the traffic identification rule is invalid.

**----End**

# 2.7.2 Configuring the Tariff Level

## Context

After identifying the traffic destined for different networks, the device associates traffic with tariff levels through traffic groups, based on which the device collects statistics and enforces policies on different types of traffic.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **traffic-group** *group-name*

A traffic group is created and the traffic group view is displayed.

By default, no traffic group exists on the device.

**Step 3** Run **acl** *acl-number* **tariff-level** *tariff-level*

The tariff level is configured.

By default, no tariff level is configured.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

- In a traffic group, you can specify tariff levels for a maximum of 8 ACLs.
- Different ACLs can share the same tariff level.
- If there is an ACL rule with both the source and destination addresses configured and the destination address is the same as that in another ACL rule, you are advised to match this ACL rule with a tariff level (*tariff-level*) with a small value during configuration. For example, most users accessing destination address A on the network use the same tariff corresponding to ACL 3000, and a small number of users with source address B and accessing destination address A use another tariff corresponding to ACL 3001. In this case, the tariff level corresponding to ACL 3001 should have a smaller value than the tariff level corresponding to ACL 3000.

**Step 4** Run **quit**

Return to the system view.

**Step 5** Run **traffic-group** *group-name* **enable**

The traffic group is applied to the device globally.

By default, no traffic group is applied to the device.

NOTE

If you modify a traffic group that has been applied, the modification takes effect only after the traffic group is applied to the device again by using this step.

- The **acl tariff-level** command changes the tariff level of traffic.
- The **rule (advanced ACL view)** command changes the source or destination address in the traffic classification rule.

**----End**

# 2.7.3 Configuring Traffic-based Accounting

## Context

Traffic-based accounting means that the authentication device collects traffic statistics during a user's online period, and sends statistics result to the accounting server. The accounting server then performs accounting for the user based on traffic statistics result. The accounting server can perform accounting based on traffic statistics result for the users going online through 802.1X, MAC address, Portal, or PPPoE authentication.

After the traffic identification rule and tariff level are configured, the device marks tariff levels on traffic from different destination addresses. Then the traffic policing and statistics functions are configured in QoS profiles to control the bandwidth and collect traffic statistics. A tariff level can identify the traffic destination address. If the specified tariff level is bound to a QoS profile, the device can control the bandwidth for the traffic destined for the specified destination address and collect the traffic statistics. If the accounting function is enabled, the device sends the traffic statistics to the accounting server for accounting.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **qos-profile** *profile-name*

A QoS profile is created and the QoS profile view is displayed.

By default, no QoS profile is configured.

**Step 3** (Optional) Run **car cir** *cir-value* [ **pir** *pir-value* ] [ **cbs** *cbs-value* **pbs** *pbs-value* ] { **inbound** | **outbound** }

Traffic policing is configured in the QoS profile.

By default, traffic policing is not configured in a QoS profile.

This step is mandatory if the bandwidth for the traffic needs to be limited.

**Step 4** Run **statistics enable**

Traffic statistics collection is enabled in the QoS profile.

By default, traffic statistics collection is disabled in a QoS profile.

**Step 5** Run **quit**

Return to the system view.

**Step 6** Run **aaa**

The AAA view is displayed.

**Step 7** Run **domain** *domain-name*

The domain view is displayed.

The device has two default domains: default and default_admin. The default domain is used by common access users and the default_admin domain is used by administrators.

**Step 8** Run **tariff-level** *tariff-level* { **qos-profile** *profile-name* | **accounting-on** } *

The QoS profile and accounting function are configured for the tariff level.

By default, the QoS profile and accounting function are not configured for the tariff level.

**----End**

# 2.7.4 Verifying the DAA Configuration

## Context

After DAA configurations are complete, you can check the configuration result.

## Procedure

- Run the **display traffic-group** { **all** | **name** *group-name* } command to view information about traffic group.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **display domain** [ **name** *domain-name* ] command to view the QoS profile bound to each tariff level and check whether the accounting function is enabled for each tariff level.

**----End**

# 2.8 Configuration Examples for DAA

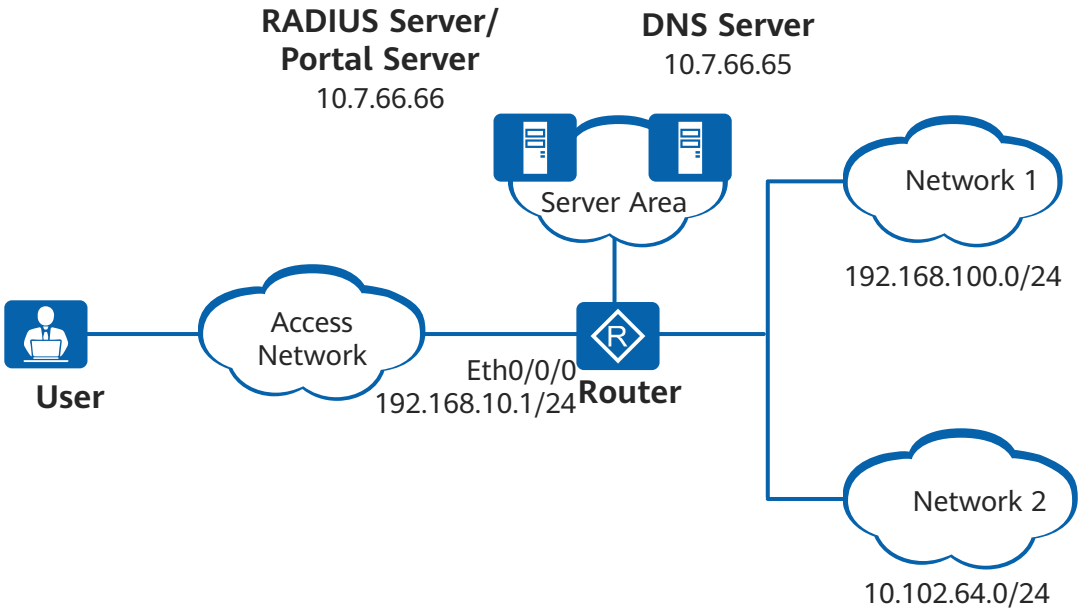
## 2.8.1 Example for Configuring Accounting for the Specified Network

### Networking Requirements

As shown in **Figure 2-3**, a Portal user on the campus network can access resources on the Network 1 (192.168.100.0/24) and Network 2 (10.102.64.0/24) through the Router. Resources on Network 1 are free and resources on Network 2 are not free. The users are charged based on traffic when they access resources on Network 2.

The DAA function needs to be configured on the Router so that the user is not charged when accessing the Network 1 and charged based on traffic when accessing the Network 2.

**Figure 2-3** Networking diagram of configuring accounting for the specified network




### Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and add interfaces to VLANs to ensure network communication.

 Copyright © Huawei Technologies Co., Ltd. 

2. Create and configure a RADIUS server template, an AAA scheme and a domain, and bind the RADIUS server template and AAA scheme to the domain, so that the device can exchange information with the RADIUS server.
3. Configure Portal authentication so that the user can access networks in Portal authentication mode.
4. Configure DAA to perform destination-based accounting.
   a. Configure the traffic identification rules for the two network segments so that the device can classify traffic going to different destination addresses.
   b. Configure different tariff levels for traffic destined for different network segments. The tariff level of traffic going to Network 1 is 1 and the tariff level of traffic going to Network 2 is 2.
   c. Configure accounting policies for tariff levels:
      - For tariff level 1, traffic statistics collection is enabled but accounting is not performed.
      - For tariff level 2, traffic statistics collection is enabled and accounting is performed.

NOTE

Ensure that the RADIUS server IP address, port number, and shared key in the RADIUS server template are configured correctly and are the same as those on the RADIUS server.

Ensure that reachable routes exist between the Router and RADIUS server, and between the user and two network segments.

## Procedure

**Step 1** Configure Eth0/0/0 that is connected to users.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] undo portswitch
[Router-Ethernet0/0/0] ip address 192.168.10.1 24
[Router-Ethernet0/0/0] quit
```

**Step 2** Configure AAA.

# Configure a RADIUS server template shiva. The IP address and port number of the RADIUS authentication server are 10.7.66.66 and 1812; the IP address and port number of the RADIUS accounting server are 10.7.66.66 and 1813. The shared key is Huawei@123.

```
[Router] radius-server template shiva
[Router-radius-shiva] radius-server authentication 10.7.66.66 1812
[Router-radius-shiva] radius-server accounting 10.7.66.66 1813
[Router-radius-shiva] radius-server shared-key cipher Huawei@123
[Router-radius-shiva] quit
```

# Configure the authentication scheme auth and set the authentication method to RADIUS authentication.

```
[Router] aaa
[Router-aaa] authentication-scheme auth
[Router-aaa-authen-auth] authentication-mode radius
[Router-aaa-authen-auth] quit
```

 Copyright © Huawei Technologies Co., Ltd. 

# Configure the accounting scheme abc and set the accounting method to RADIUS accounting.

```
[Router-aaa] accounting-scheme abc
[Router-aaa-accounting-abc] accounting-mode radius
[Router-aaa-accounting-abc] quit
```

# Configure an AAA domain huawei, and apply the authentication scheme auth, accounting scheme abc, and RADIUS server template shiva to the domain.

```
[Router-aaa] domain huawei
[Router-aaa-domain-huawei] authentication-scheme auth
[Router-aaa-domain-huawei] accounting-scheme abc
[Router-aaa-domain-huawei] radius-server shiva
[Router-aaa-domain-huawei] quit
[Router-aaa] quit
```

**Step 3** Configure DAA.

# Configure ACL 3000 and ACL 3001, which are used as traffic identification rules.

```
[Router] acl 3000
[Router-acl-adv-3000] rule 1 permit ip destination 192.168.100.0 0.0.0.255
[Router-acl-adv-3000] quit
[Router] acl 3001
[Router-acl-adv-3001] rule 1 permit ip destination 10.102.64.0 0.0.0.255
[Router-acl-adv-3001] quit
```

# Configure the tariff levels. The tariff level of traffic destined for 192.168.100.0/24 is 1 and the tariff level of traffic destined for 10.102.64.0/24 is 2.

```
[Router] traffic-group huawei
[Router-traffic-group-huawei] acl 3000 tariff-level 1
[Router-traffic-group-huawei] acl 3001 tariff-level 2
[Router-traffic-group-huawei] quit
[Router] traffic-group huawei enable
```

# Configure traffic-based accounting.

```
[Router] qos-profile huawei
[Router-qos-profile-huawei] statistics enable
[Router-qos-profile-huawei] quit
[Router] aaa
[Router-aaa] domain huawei
[Router-aaa-domain-huawei] tariff-level 1 qos-profile huawei
[Router-aaa-domain-huawei] tariff-level 2 qos-profile huawei accounting-on
[Router-aaa-domain-huawei] quit
[Router-aaa] quit
```

**Step 4** Configure Portal authentication.

# Configure the Portal server template **abc**.

```
[Router] web-auth-server abc
[Router-web-auth-server-abc] server-ip 10.7.66.66
[Router-web-auth-server-abc] port 50200
[Router-web-auth-server-abc] url http://10.7.66.66:8080/webagent
[Router-web-auth-server-abc] shared-key cipher Huawei@123
[Router-web-auth-server-abc] quit
```

# Configure the Portal access profile **web1**.

```
[Router] portal-access-profile name web1
[Router-portal-acces-profile-web1] web-auth-server abc layer3
[Router-portal-acces-profile-web1] quit
```

# Configure the authentication-free rule profile **default_free_rule** to allow packets to the DNS server to pass through.

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router] free-rule-template name default_free_rule
[Router-free-rule-default_free_rule] free-rule 1 destination ip 10.7.66.65 mask 32
[Router-free-rule-default_free_rule] quit
```

# Configure the authentication profile **p1**, bind the Portal access profile **web1** and authentication-free rule profile **default_free_rule** to the authentication profile, and specify the domain **huawei** as the forcible authentication domain in the authentication profile.

```
[Router] authentication-profile name p1
[Router-authen-profile-p1] portal-access-profile web1
[Router-authen-profile-p1] access-domain huawei force
[Router-authen-profile-p1] free-rule-template default_free_rule
[Router-authen-profile-p1] quit
```

# Bind the authentication profile **p1** to Eth0/0/0 and enable Portal authentication.

```
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] authentication-profile p1
[Router-Ethernet0/0/0] quit
```

**Step 5** Verify the configuration.

# Run the **display traffic-group name** *group-name* command to check information about the traffic group huawei.

```
[Router] display traffic-group name huawei
  ------------------------------------------------------------------------------
  Acl-id              Tariff-level
  ------------------------------------------------------------------------------
  3000                   1
  3001                   2
  ------------------------------------------------------------------------------
  Total: 2
```

**----End**

## Configuration Files

Router configuration file

```
#
 sysname Router
#
authentication-profile name p1
 portal-access-profile web1
 free-rule-template default_free_rule
 access-domain huawei force
#
radius-server template shiva
 radius-server shared-key cipher %^%#}O.80;*E;-a|55;)dmDEL;b!0YmhAPafqkV{CMf;%^%#
 radius-server authentication 10.7.66.66 1812 weight 80
 radius-server accounting 10.7.66.66 1813 weight 80
#
acl number 3000
 rule 1 permit ip destination 192.168.100.0 0.0.0.255
acl number 3001
 rule 1 permit ip destination 10.102.64.0 0.0.0.255
#
qos-profile huawei
  statistics enable
#
free-rule-template name default_free_rule
 free-rule 1 destination ip 10.7.66.65 mask 255.255.255.255
#
web-auth-server abc
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 server-ip 10.7.66.66
 port 50200
 shared-key cipher %^%#'=oP;*.KKUSPqB7M5Cf2G)!!!t/&,$!!!!!!!!!!%^%#
 url http://10.7.66.66:8080/webagent
#
portal-access-profile name web1
 web-auth-server abc layer3
#
aaa
 authentication-scheme auth
  authentication-mode radius
 accounting-scheme abc
  accounting-mode radius
 domain huawei
  authentication-scheme auth
  accounting-scheme abc
  radius-server shiva
  tariff-level 1 qos-profile huawei
  tariff-level 2 qos-profile huawei accounting-on
  statistic enable
#
interface Ethernet0/0/0
 undo portswitch
 ip address 192.168.10.1 255.255.255.0
 authentication-profile p1
#
traffic-group huawei
  acl 3000 tariff-level 1
  acl 3001 tariff-level 2
traffic-group huawei enable
#
return
```

 Copyright © Huawei Technologies Co., Ltd. 

# 3 NAC Configuration

## About This Chapter

### Context

NOTE

Network Admission Control (NAC) prevents unauthorized devices (clients) from gaining access to the network. When this function is used, Huawei will not collect or save user communication information independently. You must use the features in compliance with applicable laws and regulations, and ensure that your customers' privacy is protected when you are collecting or saving communication information as necessary.

3.1 Overview of NAC

3.2 Understanding NAC

3.3 Application Scenarios for NAC

3.4 Licensing Requirements and Limitations for NAC

3.5 Default Settings for NAC

3.6 Configuring NAC

3.7 Maintaining NAC

3.8 Configuration Examples for NAC

3.9 FAQ

## 3.1 Overview of NAC

### Definition

Network Admission Control (NAC) is an end-to-end security control technology that authenticates clients and users who attempt to access the network.

With the development of enterprise network, threats increasingly bring risks, such as viruses, Trojan horses, spyware, and malicious network attacks. On a traditional enterprise network, the intranet is considered as secure and threats come from

 Copyright © Huawei Technologies Co., Ltd. 

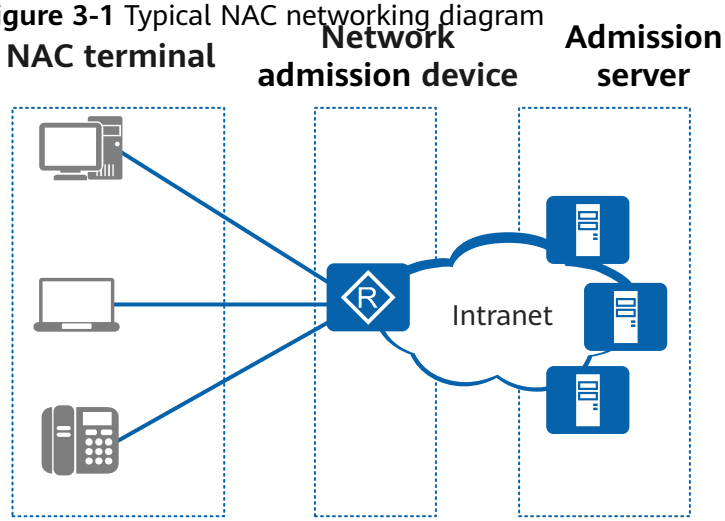
extranet. However, 80% security threats actually come from the intranet. The intranet threats will cause serious damage in a wide range. Even worse, the system and network will break down. In addition, when intranet users browse websites on the external network, the spyware and Trojan horse software may be automatically installed on users' computers, which cannot be sense by the users. The malicious software may spread on the internal network.

The traditional security measures cannot meet requirements on border defense due to increasing security challenges. The security model should be converted into active mode to solve security problems from the roots (terminals), improving information security level of the entire enterprise.

The NAC solution integrates terminal security and access control and takes the check, audit, secure, and isolation measures to improve the proactive protection capability of terminals. This solution ensures security of each terminal and the entire enterprise network.

As shown in **Figure 3-1**, NAC includes three components: NAC terminal, network access device, and access server.

**Figure 3-1** Typical NAC networking diagram




- NAC terminal: functions as the NAC client and interacts with network access devices to authenticate access users. If 802.1X authentication is used, users must install client software.
- Network access device: function as the network access control point that enforces enterprise security policies. It allows, rejects, isolates, or restricts users based on the security policies customized for enterprise networks.
- Access server: includes the access control server, management server, antivirus server, and patch server. It authenticates users, checks terminal security, repairs and upgrades the system, and monitors and audits user actions.

## Purpose

Traditional network security technologies focus on threats from external computers, but typically neglect threats from internal computers. In addition, current network devices cannot prevent attacks initiated by devices on internal networks.

 Copyright © Huawei Technologies Co., Ltd. 

The NAC security framework was developed to ensure the security of network communication services. The NAC security framework improves internal network security by focusing on user terminals, and implement security control over access users to provide end-to-end security.

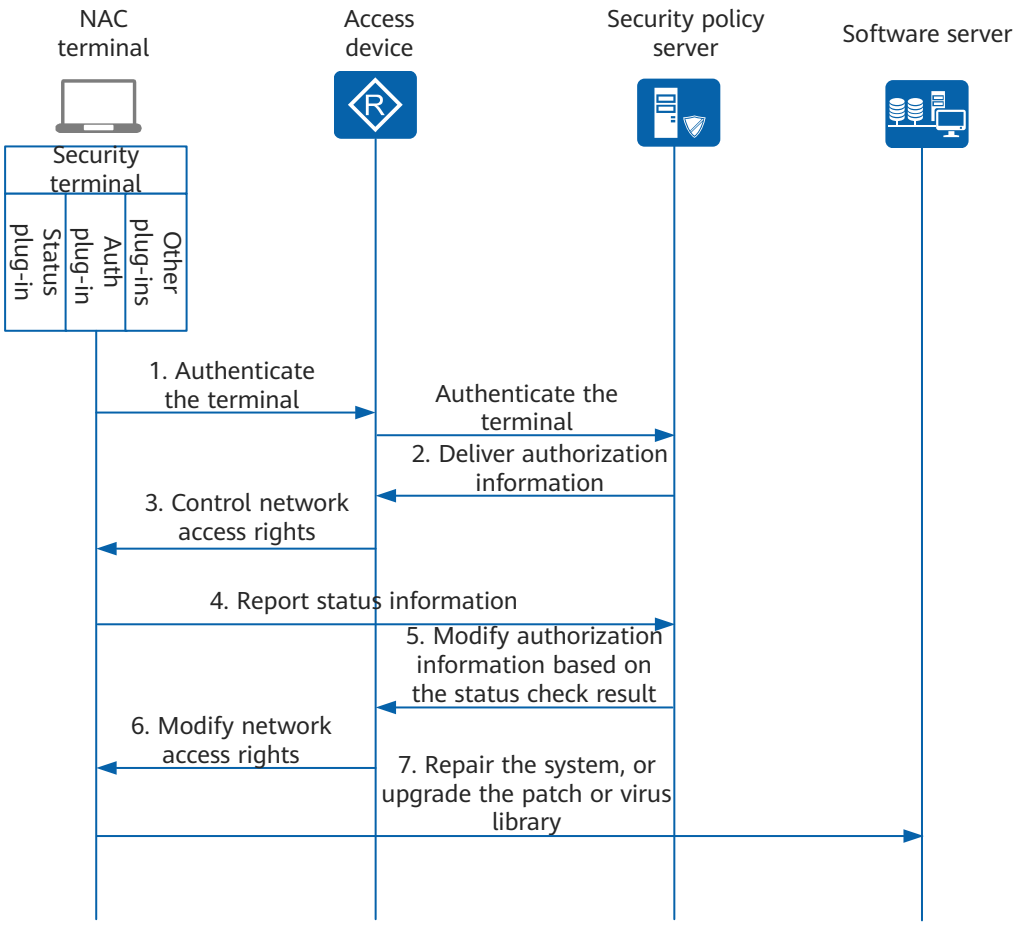
# 3.2 Understanding NAC

## 3.2.1 NAC Fundamentals

### Process

Figure 3-2 shows the basic NAC process.

**Figure 3-2** Basic NAC process




1. The access device works with a security policy server (for example, an AAA server) to authenticate the user when an NAC terminal connects to the network.

 Copyright © Huawei Technologies Co., Ltd. 

2. The security policy server delivers the authorization information to the access device if the user is authenticated. If the authentication fails, the access device isolates the user.
3. Based on the authorization information from the security policy server, the access device controls the terminal user's network access rights and establishes a communication channel between the terminal and security policy server.
4. The NAC terminal directly exchanges information with the security policy server. The terminal reports its status information, including the antivirus database, operating system, and patch versions.
5. The security policy server checks the terminal status, and redelivers the authorization information to the access device if the NAC terminal does not comply with enterprise security standards.
6. The access device modifies the terminal user's network access rights according to the authorization information delivered by the security policy server.
7. Based on the status check result, the NAC terminal connects to the software server to download client software, repair the system, or upgrade the patch or antivirus database until the terminal complies with the enterprise security standards.

## Comparison Between Three Authentication Modes

NAC provides three authentication modes: 802.1X authentication, MAC address authentication, and Portal authentication. **Table 3-1** compares the three authentication modes.

**Table 3-1** Authentication mode comparisons

| Item | 802.1X Authentication | MAC Address Authentication | Portal Authentication |
| --- | --- | --- | --- |
| Client | Required | Not required | Not required |
| Advantage | High security | No client required | Flexible deployment |
| Disadvantage | Inflexible deployment | Complex management and MAC address registration required | Low security |
| Scenario | New network with concentrated users and high requirements for security | Authentication of dumb terminals such as printers and fax machines | Scenario with flexible authentication modes and scattered users |

 Copyright © Huawei Technologies Co., Ltd. 

# 3.2.2 802.1X Authentication

## Overview

To resolve wireless local area network (LAN) security issues, the Institute of Electrical and Electronics Engineers (IEEE) 802 LAN/wide area network (WAN) committee developed the 802.1X protocol. Later, the 802.1X protocol was widely applied as a common access control mechanism on LAN interfaces for authentication and security on Ethernet networks.

The 802.1X protocol is an interface-based network access control protocol. It controls users' access to network resources by authenticating the users on access interfaces.

As shown in **Figure 3-3**, an 802.1X system uses a standard client/server architecture with three components: client, access device, and authentication server.

**Figure 3-3** Diagram of the 802.1X authentication system




- Client: an entity on the LAN segment, which is authenticated by the access device on the same LAN segment. The client is usually a user terminal. The user triggers 802.1X authentication using client software. The client must support Extensible Authentication Protocol over LAN (EAPoL).
- Access device: an entity on the LAN segment, which authenticates the connected client. The access device is usually a network device that supports the 802.1X protocol. The device provides an interface for the client to access the LAN.
- Authentication server: an entity that provides the authentication service for the access device. The authentication server, which is usually a RADIUS server, carries out authentication, authorization, and accounting on users.

## Authentication Triggering Modes

802.1X authentication can be initiated by either the client or access device. The device supports the following authentication triggering modes:

1. Triggered by the client: A user starts the client and enters the user name and password. The client then sends an EAP packet to the access device to trigger authentication.
2. Triggered by the access device: When receiving a DHCP/ARP packet from a user terminal, the access device proactively enables the user terminal to display the client page and prompt the user to enter the user name and password. After the user name and password are entered, the authentication is started.

 Copyright © Huawei Technologies Co., Ltd. 

## Authentication Modes

In an 802.1X authentication system, the client, access device, and authentication server exchange authentication information using the Extensible Authentication Protocol (EAP). The EAP packet exchange process is described as follows:

1. The EAP packets transmitted between the client and access device are encapsulated in EAPoL format and transmitted across the LAN.
2. The access device and authentication server (for example, a RADIUS server) exchange EAP packets in the following modes:
   - EAP relay: The access device relays EAP packets. The device encapsulates EAP packets in EAP over RADIUS (EAPoR) format and sends the packets to the RADIUS server for authentication. This authentication mode simplifies device processing and supports various EAP authentication methods, such as MD5-Challenge, EAP-TLS, and PEAP. However, the RADIUS server is required to support corresponding authentication methods.
   - EAP termination: The access device terminates EAP packets. The device encapsulates client authentication information into standard RADIUS packets, which are then authenticated by the server using the Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). This authentication mode is applicable since mainstream RADIUS servers support PAP and CHAP authentication and server update is unnecessary. However, device processing is complex, and the device supports only the MD5-Challenge EAP authentication method.

NOTE

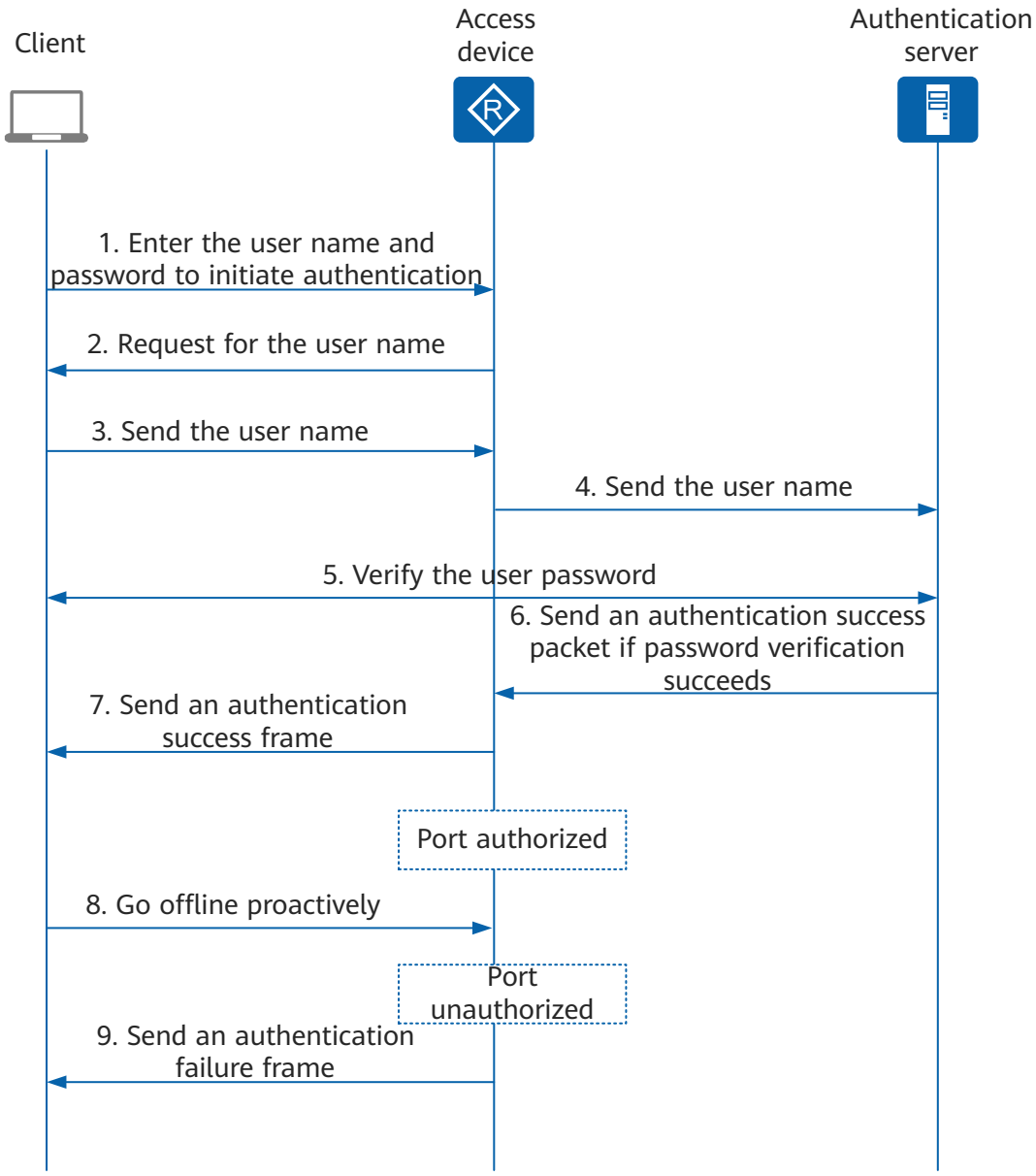
The device supports the following EAP protocols: EAP-TLS, EAP-TTLS, EAP-PAP, EAP-CHAP (EAP-MD5), and EAP-PEAP.

## Authentication Process

**Figure 3-4** shows the 802.1X authentication process in EAP relay mode.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 3-4** Service process in EAP relay mode




1. When a user needs to access an external network, the user starts the 802.1X client program, enters the applied and registered user name and password, and initiates a connection request. At this time, the client sends an authentication request packet to the device to start the authentication process.
2. After receiving the authentication request packet, the device sends a user name request packet, requesting the client to send the previously entered user name.
3. In response to the request sent by the device, the client sends the user name to the device.

 Copyright © Huawei Technologies Co., Ltd. 

4. The device sends the user name to the authentication server for processing.
5. After receiving the user name forwarded by the device, the authentication server verifies the user password.
   a. The authentication server uses the user name to search the user name list in the database to find the corresponding user password.
   b. The authentication server encrypts the password with a randomly generated MD5 challenge, and sends the MD5 challenge to the client through the access device.
   c. After receiving the MD5 challenge from the device, the client encrypts the password with the MD5 challenge and sends the encrypted password to the authentication server through the access device.
   d. The authentication server compares the encrypted password received and the locally encrypted password. If the two passwords are the same, the user is considered authorized; if they are different, the user is considered unauthorized.
6. After the password verification succeeds, the authentication server sends an authentication success packet to the access device.
7. After receiving the authentication success packet, the device sends a packet indicating that the authentication is successful to the client, changes the interface status to authorized, and allows the user to access the network through the interface.
8. If the user wants to go offline, the client sends a logoff packet to the device.
9. The access device changes the interface status from authorized to unauthorized. It sends an authentication failure packet to the client and concurrently deletes the user login information.

Steps 4 and 5 are different in the authentication processes in EAP termination and relay modes. In EAP termination mode, when sending the user name from the client to the authentication server, the access device randomly generates an MD5 challenge to the client. (In this mode, the MD5 challenge is not generated by the authentication server.) The access device then sends the user name, MD5 challenge, and encrypted password to the authentication server for processing.

## 3.2.3 MAC Address Authentication

### Overview

MAC address authentication controls a user's network access rights based on the user's interface and MAC address. The user does not need to install any client software. The device starts authenticating a user when detecting the user's MAC address for the first time on the interface where MAC address authentication has been enabled. During the authentication process, the user does not need to enter a user name or password.

### User Name Format

Based on different user name formats and content that the access device uses to authenticate users, user name formats used in MAC authentication can be classified into the following types:

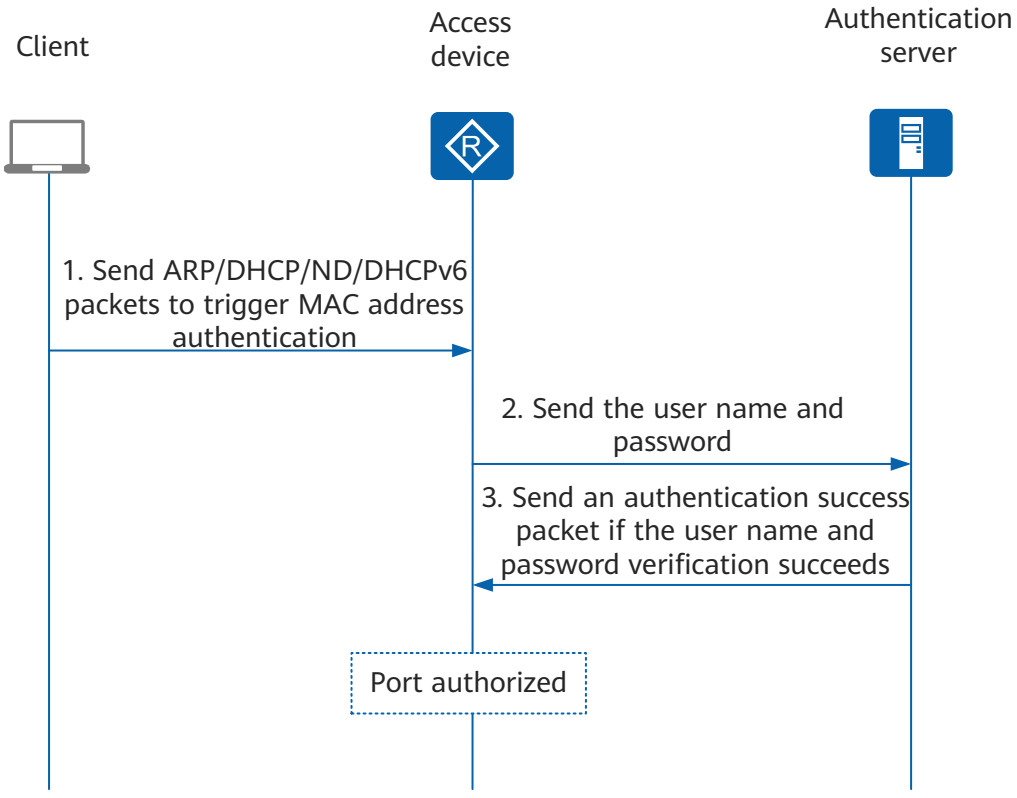
 Copyright © Huawei Technologies Co., Ltd. 

- MAC address: The device uses a user's MAC address as the user name for authentication. The device can also use the MAC address or a user-defined character string as the user password.
- Fixed user name: Regardless of users' MAC addresses, all users use a fixed name and password designated on the access device for authentication. As multiple users can be authenticated on the same interface, all users requiring MAC address authentication on the interface use the same fixed user name. The server only needs to configure one user account to meet the authentication demands of all users. This applies to a network environment with reliable clients.
- DHCP option: The device replaces a user's MAC address with the obtained user DHCP option and a fixed password as identity information for authentication. In this mode, the device must support MAC authentication triggering through DHCP packets.

## Authentication Process

**Figure 3-5** shows the MAC authentication process.

**Figure 3-5** MAC address authentication process




1. The device triggers MAC address authentication for a user when detecting any ARP/DHCP/ND/DHCPv6 packet sent by the user.
2. Based on the configuration, the device sends the user name and password to the authentication server for authentication.


Copyright © Huawei Technologies Co., Ltd.

3. The authentication server verifies the received user name and password. If the verification succeeds, the server sends an authentication success packet to the device. After receiving the authentication success packet, the device changes the interface status to authorized and allows the user to access the network through the interface.

## 3.2.4 Portal Authentication

### Overview

Portal authentication is also called web authentication. Generally, Portal authentication websites are also called Portal websites. When users go online, they must be authenticated on Portal websites. The users can use network resources only after they pass the authentication.

A user can access a known Portal authentication website and enter a user name and password for authentication. This mode is called active authentication. If a user attempts to access other external networks through HTTP, the device forcibly redirects the user to the Portal authentication website for Portal authentication. This mode is called forcible authentication.

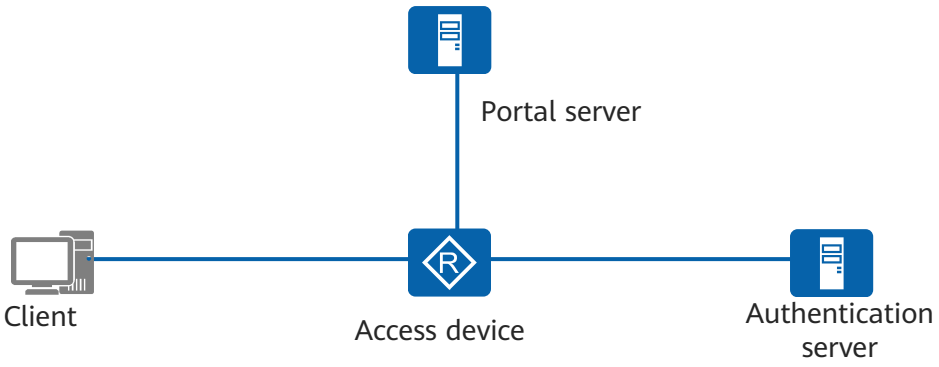
### System Architecture

A Portal server can be an external Portal server, or a built-in Portal server.

- **Using an external Portal server**

As shown in **Figure 3-6**, typical networking of a Portal authentication system using an external Portal server consists of four entities: client, access device, Portal server, and authentication server.

**Figure 3-6** Portal authentication system using an external Portal server




1. Client: has a browser running HTTP installed.
2. Access device: includes switches and routers, and provides the following functions:
   - Redirects all HTTP requests from users on authentication subnets to the Portal server before authentication.
   - Interacts with the Portal server and authentication server to implement identity authentication, authorization, and accounting during authentication.

 Copyright © Huawei Technologies Co., Ltd. 

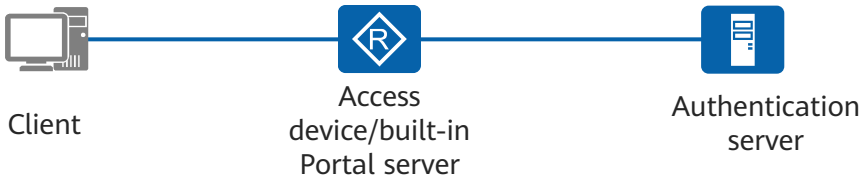
  - Allows the users to access authorized Internet resources after the authentication succeeds.

3. Portal server: receives authentication requests from clients, provides free Portal services and authentication pages, and exchanges the client authentication information with the access device.
4. Authentication server: interacts with the access device to implement user authentication, authorization, and accounting.

- **Using a built-in Portal server**

The access device with the built-in Portal server implements the Portal server functions. In this scenario, the Portal authentication system only includes three entities: client, access device, and authentication server, as shown in **Figure 3-7**.

**Figure 3-7** Portal authentication system using a built-in Portal server




The built-in Portal server provides Portal authentication, without the need to deploy an extra Portal server.

The device with a built-in Portal server implements basic Portal server functions and only provides web-based login and logout functions for users. It cannot completely replace an independent Portal server or support any extended functions of an external server.

## Authentication Modes

Different Portal authentication modes can be used in different networking modes. Portal authentication is classified into Layer 2 authentication and Layer 3 authentication according to the network layer on which it is implemented.

- **Layer 2 authentication**

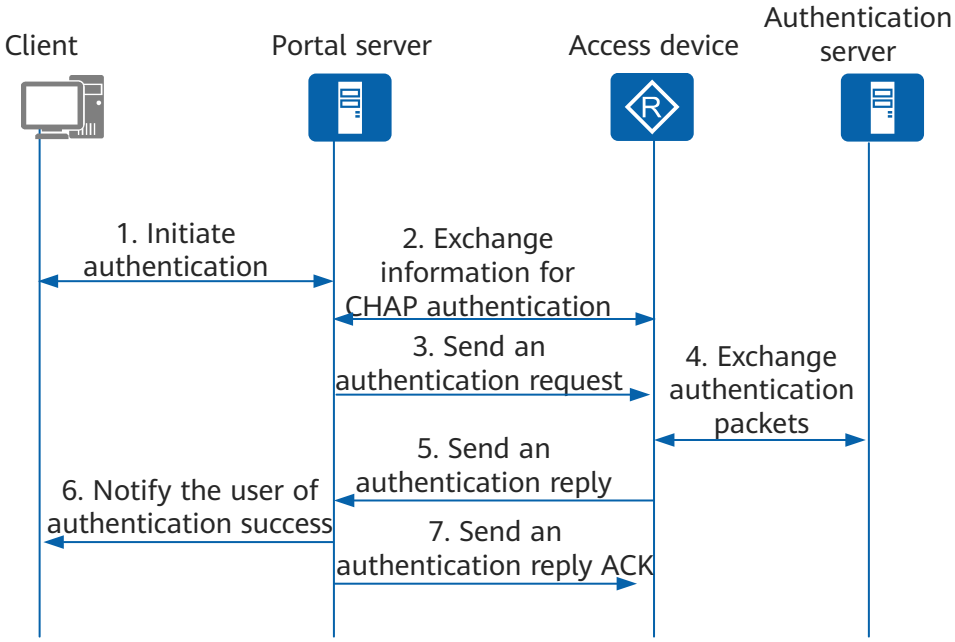
The client and access device are either directly connected or have only Layer 2 devices between them. The device can learn users' MAC addresses and identify the users using their MAC addresses and IP addresses. On a network of this configuration, Layer 2 authentication should be used.

Layer 2 authentication provides a simple authentication process with high security. However, users must be in the same network segment with the access device, which makes the networking inflexible.

**Figure 3-8** shows the packet interaction process in Layer 2 authentication.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 3-8** Layer 2 authentication process of the Portal protocol

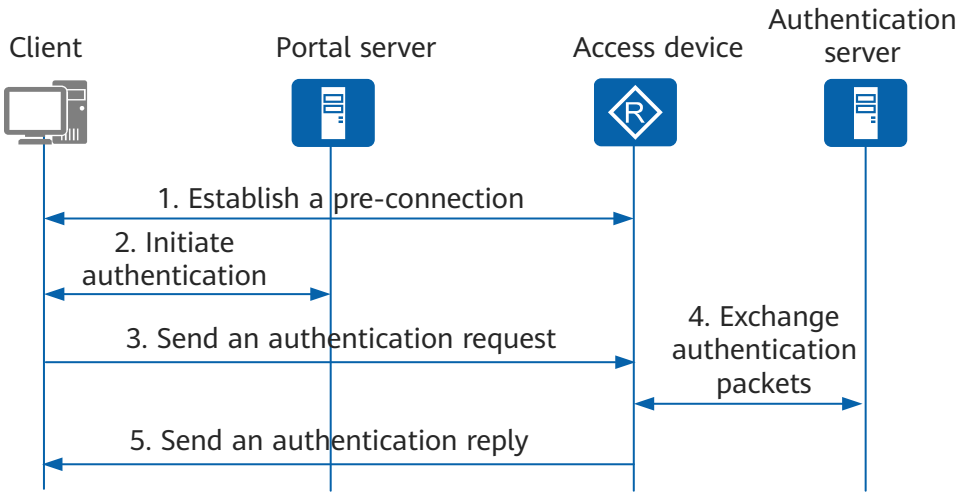



1. The user initiates an authentication request through HTTP. The access device allows an HTTP packet destined for the Portal server or an HTTP packet destined for the configured authentication-free network resources to pass. The access device redirects HTTP packets accessing other addresses to the Portal server. The Portal server provides a web page on which the user must enter the user name and password for authentication.
2. The Portal server exchanges information with the access device to implement Challenge Handshake Authentication Protocol (CHAP) authentication. If Password Authentication Protocol (PAP) authentication is used, the Portal server directly performs step 4 without exchanging information with the access device.
3. The Portal server sends the user name and password entered by the user to the access device through an authentication request packet.
4. The access device exchanges authentication packets with the authentication server.
5. The access device sends an authentication reply packet to the Portal server.
6. The Portal server sends an authentication success packet to the client, notifying the client that the authentication succeeded.
7. The Portal server sends an authentication reply ACK packet to the access device.

or an external Portal server, authentication processes of different authentication protocols are different. **Figure 3-8** shows the authentication process of the Portal protocol. **Figure 3-9** shows the authentication process of the HTTP or HTTPS protocol.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 3-9** Layer 2 authentication process of the HTTP or HTTPS protocol




1. Before authentication, a pre-connection is established between the client and device.
2. The client initiates an authentication request using HTTP or HTTPS. The access device allows an HTTP or HTTPS packet destined for the Portal server or an HTTP or HTTPS packet destined for the configured authentication-free network resources to pass through. The access device redirects HTTP or HTTPS packets accessing other addresses to the Portal server. The Portal server provides a web page on which the user must enter the user name and password for authentication, and instructs the client to send a POST authentication request packet to the access device.
3. The client encapsulates the user name and password into a POST authentication request packet and sends the packet to the access device.
4. The access device and authentication server exchange authentication packets.
5. The access device sends an authentication reply packet to the client.

- **Layer 3 authentication**

When the device is deployed at the aggregation or core layer, Layer 3 forwarding devices exist between the client and device. In this scenario, the device may not obtain the MAC address of the client. Therefore, the device only uses the IP address to identify the user. On a network of this configuration, Layer 3 authentication should be used.

The Layer 3 authentication process is similar to the Layer 2 authentication process, except that a pre-connection is established between the client and access device in Layer 3 authentication. Networking of the Layer 3 authentication is flexible, which facilitates remote control. However, only an IP address can be used to identify a user, so Layer 3 authentication has low security.

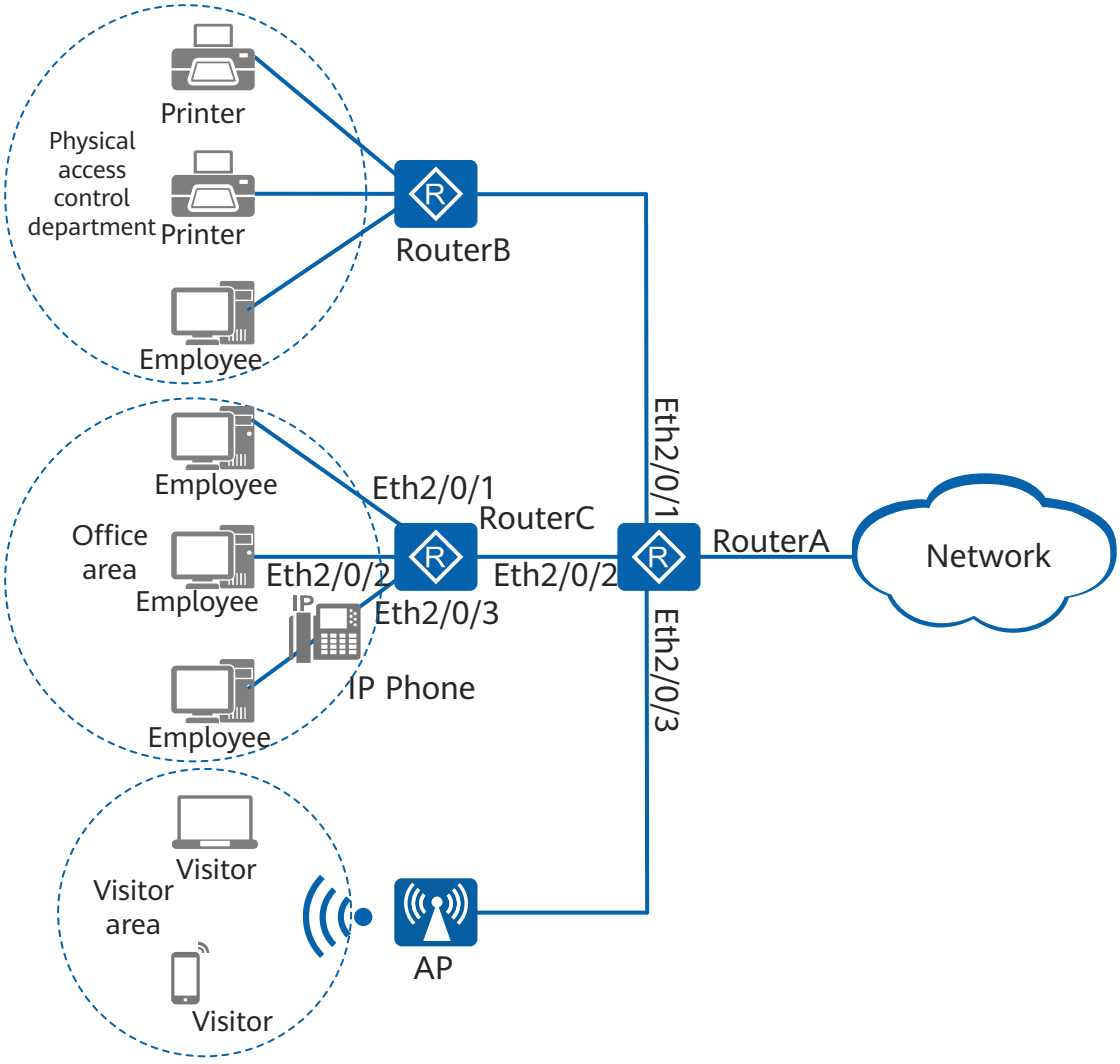
# 3.3 Application Scenarios for NAC

On the network shown in **Figure 3-10**, the physical access control department of an enterprise is connected to RouterA through RouterB, the office area is connected to RouterA through RouterC, and the visitor area is connected to

 Copyright © Huawei Technologies Co., Ltd. 

RouterA through an AP. To ensure security of the enterprise intranet, network access of the users needs to be controlled. Only the users who pass authentication are authorized to access specified network resources.

**Figure 3-10** Using NAC to control network access of enterprise users




In the physical access control department, there are terminals of multiple types and the number of printers is greatly more than that of employees. Therefore, deploy 802.1X authentication and MAC address authentication (triggered first) on Eth2/0/1 of RouterA, and configure the user access mode to multi-authen.

The office area has high security requirements. Therefore, deploy 802.1X authentication on RouterC's Eth2/0/1 and Eth2/0/2 connected only to PCs, and configure the user access mode to single-terminal. At the same time, deploy 802.1X authentication and MAC address authentication on Eth2/0/3 connected to IP phones and PCs, and configure the user access mode to single-voice-with-data.

In the visitor area, users move frequently and have low network access rights. Therefore, deploy Portal authentication on Eth2/0/3 of RouterA, and configure the user access mode to multi-share.


Copyright © Huawei Technologies Co., Ltd.

# 3.4 Licensing Requirements and Limitations for NAC

## Involved Network Elements

**Table 3-2** Components involved in NAC networking

| Role | Product Model | Description |
| --- | --- | --- |
| AAA server | Huawei servers or third-party AAA servers | Performs authentication, accounting, and authorization on users. |
| Portal server | Huawei servers or third-party Portal servers | Receives authentication requests from Portal clients, provides free portal services and an interface based on web authentication, and exchanges authentication information of the authentication clients with access devices.<br>This component is required only in external Portal authentication mode. |

## Licensing Requirements

NAC is a basic feature of the device and is not under license control.

## Feature Limitations

When deploying NAC on the router, pay attention to the following:

- The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support NAC.
- You can run the **display access-user user-id** command to view rate limiting parameter values delivered by the RADIUS server. If only the CIR value for rate limiting is set on the RADIUS server and other rate limiting parameter values (CBS or PBS value) are not set, the access control device obtains other parameter values based on empirical value verification.

  The parameter values obtained by the access control device after it verifies rate limiting parameters delivered by the RADIUS server differ from those obtained by the device after it verifies rate limiting parameters delivered by the QoS profile.
- If a terminal uses Portal authentication or multi-mode authentication (including Portal authentication), the device cannot grant VLAN-based


Copyright © Huawei Technologies Co., Ltd.

authorization to the terminal. If a terminal obtains VLAN-based authorization, you need to manually trigger the DHCP process to request an IP address.

- If a terminal has both IPv4 and IPv6 addresses, only the IPv4 address can be used for user detection and update of the user entry corresponding to the IPv6 address. The IPv6 address cannot be used for update of the user entry corresponding to the IPv4 address.
- In the Portal authentication scenario, users may use spoofed IP addresses for authentication, which brings security risks. It is recommended that you configure attack defense functions such as IPSG and DHCP snooping to avoid the security risks.

# 3.5 Default Settings for NAC

## 802.1X Access Profile

The system provides a predefined 802.1X access profile named **dot1x_access_profile**. Table 3-3 lists the default settings for an 802.1X access profile created on the device.

**Table 3-3** Default settings for an 802.1X access profile

| Parameter | Default Setting |
| --- | --- |
| Authentication mode of 802.1X users | EAP authentication |
| Actively initiating 802.1X authentication | Enabled |
| Handshake with online users | Disabled |
| Re-authentication for online 802.1X users | Disabled |
| Retransmissions count of authentication request packets | 2 |
| Client authentication timeout interval | 5 seconds |
| Timeout interval of an authentication request | 30 seconds |

## MAC Access Profile

The system provides a predefined MAC access profile named **mac_access_profile**. Table 3-4 lists the default settings for a MAC access profile created on the device.


Copyright © Huawei Technologies Co., Ltd.

**Table 3-4** Default settings for a MAC access profile

| Parameter | Default Setting |
| --- | --- |
| User name and password format for MAC address authentication | MAC addresses without hyphens (-) |
| Types of packets that can trigger MAC address authentication | DHCP, ARP, DHCPv6, and ND packets |
| Re-authentication for online MAC address authentication users | Disabled |
| Re-authentication interval for online MAC address authentication users | 1800 seconds |
| Re-authentication for users upon receipt of DHCP lease renewal packets | Disabled |

## Portal Access Profile

The system provides a predefined Portal access profile named **portal_access_profile**. Table 3-5 lists the default settings for a Portal access profile created on the device.

**Table 3-5** Default settings for a Portal access profile

| Parameter | Default Setting |
| --- | --- |
| Portal server | Unspecified |
| Source network segment for Portal authentication | All network segments |
| User offline detection interval | 300 seconds |
| Escape authorization (network access rights assigned to users when the access device detects that the Portal server is Down) | Unspecified |
| Re-authentication for users when the access device detects that the Portal server state changes from Down to Up | Disabled |

## Authentication Profile

The system provides five predefined authentication profiles: default_authen_profile, dot1x_authen_profile, mac_authen_profile, portal_authen_profile, and dot1xmac_authen_profile. Table 3-6 lists the default settings for an authentication profile created on the device.


Copyright © Huawei Technologies Co., Ltd.

**Table 3-6** Default settings for an authentication profile

| Parameter | Default Setting |
| --- | --- |
| Access profile type and name | Unspecified |
| User access mode | **multi-authen** |
| Interval for re-authenticating users in pre-connection state | 60 seconds |

# 3.6 Configuring NAC

## 3.6.1 Configuration Procedure for NAC

### Pre-configuration Tasks

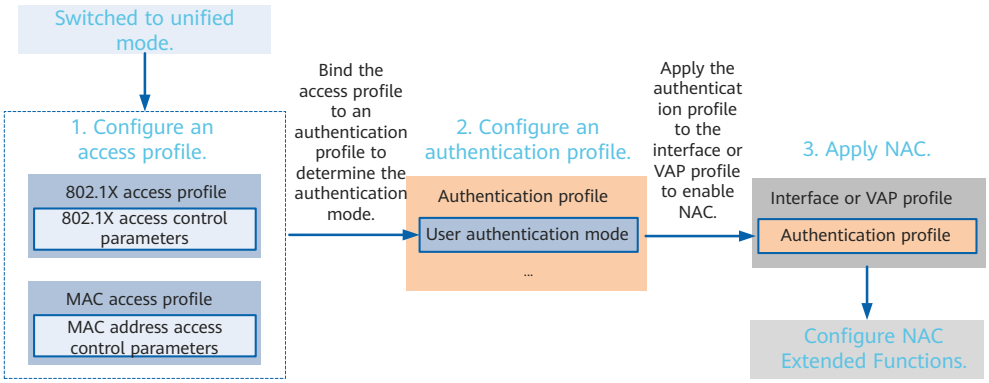
NAC only provides multiple network access control protocols for users. To completely authenticate user identity and control users' network access rights, complete the following AAA configuration tasks before configuring NAC:

- Configure the domain and AAA scheme.
- Configure the user name and password on the RADIUS or HWTACACS server if RADIUS or HWTACACS authentication is used.
- Configure the user name and password on the network access device if local authentication is used.

For details about how to configure the AAA client, see **AAA Configuration**.

### Configuration Procedure

**Figure 3-11** NAC Configuration Procedure




 Copyright © Huawei Technologies Co., Ltd. 

## NAC Configuration Tasks

| Authentication Mode | Scenario | Task |
| --- | --- | --- |
| 802.1X authentication | Users are densely distributed and high information security is required. | Perform the following configurations in sequence:<br>1. **3.6.2.1 Configuring an 802.1X Access Profile**<br>2. **3.6.3 Configuring an Authentication Profile**<br>3. **3.6.4 NAC Application** |
| MAC Address authentication | Dumb terminals such as printers and fax machines need to connect to the network. | Perform the following configurations in sequence:<br>1. **3.6.2.2 Configuring a MAC Access Profile**<br>2. **3.6.3 Configuring an Authentication Profile**<br>3. **3.6.4 NAC Application** |
| Multi-mode authentication | The device allows multiple authentication modes to be deployed simultaneously to meet various authentication requirements on the network.<br>To configure multi-mode authentication of several authentication modes, you only need to bind corresponding access profiles to an authentication profile. | Perform the following configurations in sequence:<br>1. **3.6.2 Configuring an Access Profile**<br>2. **3.6.3 Configuring an Authentication Profile**<br>3. **3.6.4 NAC Application** |


Copyright © Huawei Technologies Co., Ltd.

# 3.6.2 Configuring an Access Profile

## 3.6.2.1 Configuring an 802.1X Access Profile

### 3.6.2.1.1 Creating an 802.1X Access Profile

## Context

The device uses 802.1X access profiles to uniformly manage 802.1X access configurations. Before configuring 802.1X authentication, you need to create an 802.1X access profile.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **dot1x-access-profile name** *access-profile-name*

An 802.1X access profile is created and the 802.1X access profile view is displayed.

By default, the device has a built-in 802.1X access profile named dot1x_access_profile.

NOTE

- The device supports a maximum of 8 configurable 802.1X access profiles. The compatibility profile converted after an upgrade is not counted in the configuration specification. The built-in 802.1X access profile dot1x_access_profile can be modified and applied, but cannot be deleted.
- Before deleting an 802.1X access profile, ensure that this profile is not bound to any authentication profile.

**----End**

### 3.6.2.1.2 (Optional) Configuring an Authentication Mode for 802.1X Users

## Context

During 802.1X authentication, users exchange authentication information with the device using EAP packets. The device uses two modes to exchange authentication information with the RADIUS server.

- EAP termination: The device directly parses EAP packets, encapsulates user authentication information into a RADIUS packet, and sends the packet to the RADIUS server for authentication. EAP termination is classified into PAP or CHAP authentication.
  - PAP: The device arranges the MAC address, shared key, and random value in sequence, performs hash processing on them using the MD5 algorithm, and encapsulates the hash result into the User-Password attribute.
  - CHAP: The device arranges the CHAP ID, MAC address, and random value in sequence, performs hash processing on them using the MD5 algorithm, and encapsulates the hash result into the CHAP-Password and CHAP-Challenge attributes.

 Copyright © Huawei Technologies Co., Ltd. 

- EAP relay (specified by **eap**): The device encapsulates EAP packets into RADIUS packets and sends the RADIUS packets to the RADIUS server. The device does not parse the received EAP packets but encapsulates them into RADIUS packets. This mechanism is called EAP over Radius (EAPoR).

The processing capability of the RADIUS server determines whether EAP termination or EAP relay is used. If the RADIUS server has a higher processing capability and can parse a large number of EAP packets before authentication, the EAP relay mode is recommended. If the RADIUS server has a processing capability not good enough to parse a large number of EAP packets and complete authentication, the EAP termination mode is recommended and the device parses EAP packets for the RADIUS server. When the authentication packet processing method is configured, ensure that the client and server both support this method; otherwise, the users cannot pass authentication.

NOTE

- The EAP relay can be configured for 802.1X users only when RADIUS authentication is used.
- If AAA local authentication is used, the authentication mode for 802.1X users can only be set to EAP termination.
- Because mobile phones do not support EAP termination mode (PAP and CHAP), the 802.1X authentication + local authentication mode cannot be configured for mobile phones. Terminals such as laptop computers support EAP termination mode only after having third-party clients installed.
- If the 802.1X client uses the MD5 encryption mode, the user authentication mode on the device can be set to EAP or CHAP; if the 802.1X client uses the PEAP authentication mode, the authentication mode on the device can be set to EAP.
- In a wireless access scenario, if WPA or WPA2 authentication mode is configured in the security policy profile, 802.1X authentication does not support pre-authentication domain-based authorization.
- If an interface has online 802.1X users and the authentication mode is changed between EAP termination and EAP relay in the 802.1X access profile bound to the interface, the online 802.1X users will be logged out. If the authentication mode is changed between CHAP and PAP in EAP termination mode, the online 802.1X users will not be logged out.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **dot1x-access-profile name** *access-profile-name*

The 802.1X access profile view is displayed.

**Step 3** Run **dot1x authentication-method** { **chap** | **pap** | **eap** }

An authentication mode is configured for 802.1X users.

The default 802.1X authentication mode is **eap**, which indicates Extensible Authentication Protocol (EAP) relay authentication.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

### 3.6.2.1.3 (Optional) Configuring the Packet Types That Can Trigger 802.1X Authentication

## Context

After 802.1X authentication is enabled, the device can trigger 802.1X authentication on users by default when receiving DHCP or ARP packets. Based on user information on the actual network, the administrator can adjust the packet types that can trigger 802.1X authentication. For example, if all users on a network dynamically obtain IPv4 addresses, the device can be configured to trigger 802.1X authentication only through DHCP packets. This prevents the device from continuously sending ARP packets to trigger 802.1X authentication when static IPv4 addresses are configured for unauthorized users on the network, and reduces device CPU occupation.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **dot1x-access-profile name** *access-profile-name*

The 802.1X access profile view is displayed.

**Step 3** Run **authentication trigger-condition** { **dhcp** | **arp** } *

The packet types that can trigger 802.1X authentication are configured.

By default, DHCP/ARP packets can trigger 802.1X authentication.

**----End**

### 3.6.2.1.4 (Optional) Configuring the Authorization State of an Interface

## Context

You can configure the authorization state of an interface to control whether an access user must be authenticated before accessing network resources. The interface supports the following authentication states:

- Auto mode: The interface is initially in Unauthorized state and sends and receives EAPoL packets only. Users cannot access network resources. After a user passes the authentication, the interface turns to Authorized state. Users are allowed to access network resources in this state.
- Authorized-force mode: The interface is always in Authorized state and allows users to access network resources without authentication.
- Unauthorized-force mode: The interface is always in Unauthorized state and does not allow users to access network resources.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 2** Run **dot1x-access-profile name** *access-profile-name*

The 802.1X access profile view is displayed.

**Step 3** Run **dot1x port-control** { **auto** | **authorized-force** | **unauthorized-force** }

The authorization state of the interface is configured.

By default, the authorization state of an interface is **auto**.

**----End**

### 3.6.2.1.5 (Optional) Configuring the Device to Send EAP Packets with a Code Number to 802.1X Users

## Context

When a non-Huawei device used as the RADIUS server sends RADIUS packets with attribute 61, EAP packet code number 0xa (hexadecimal notation, 10 in decimal notation), and data type being 0x19 (hexadecimal notation, 25 in decimal notation) to the device, run the **dot1x eap-notify-packet** command on the device so that the device can send EAP packets with code number 0xa and data type 0x19 to users. If the **dot1x eap-notify-packet** command is not executed, the device does not process EAP packets of this type and users are disconnected.

Perform this configuration if the device connects to an H3C iMC RADIUS server.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **dot1x-access-profile name** *access-profile-name*

The 802.1X access profile view is displayed.

**Step 3** Run **dot1x eap-notify-packet eap-code** *code-number* **data-type** *type-number*

The device is configured to send EAP packets with a code number to 802.1X users.

By default, the device does not send EAP packets with a code number to 802.1X users.

NOTE

If an H3C iMC functions as the RADIUS server, run the **dot1x eap-notify-packet eap-code 10 data-type 25** command on the device.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

### 3.6.2.1.6 (Optional) Configuring Re-authentication for Online 802.1X Authentication Users

## Context

If the administrator modifies parameters such as access rights and authorization attributes of an online user on the authentication server, the user must be re-authenticated to ensure user validity.

If re-authentication is configured for online 802.1X authentication users, the device sends saved authentication parameters of an online user to the authentication server for re-authentication. The device saves user authentication information after users go online. If the user authentication information on the authentication server remains unchanged, the user keeps online. If the information has been modified, the user is disconnected and needs to be re-authenticated.

The device re-authenticates 802.1X authentication users in the following modes:

- The device periodically re-authenticates users using a specified 802.1X access profile.

  NOTE

  After this function is configured, many 802.1X authentication logs will be generated.

- The device is manually configured to re-authenticate a user with a specified MAC address once.

If the device is connected to a server for re-authentication and the server replies with a re-authentication deny message that makes an online user go offline, it is recommended that you locate the cause of the re-authentication failure on the server or disable the re-authentication function on the device.

## Procedure

- Configuring periodic re-authentication
  a. Run **system-view**

     The system view is displayed.
  b. Run **dot1x-access-profile name** *access-profile-name*

     The 802.1X access profile view is displayed.
  c. Run **dot1x reauthenticate**

     Re-authentication is configured for online 802.1X authentication users.

     By default, re-authentication is not configured for online 802.1X authentication users.
  d. (Optional) Run **dot1x timer reauthenticate-period** *reauthenticate-period-value*

     The re-authentication interval is configured for online 802.1X authentication users.

     By default, the re-authentication interval is 3600 seconds for online 802.1X authentication users.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

It is recommended that the re-authentication interval be set to the default value. If multiple ACLs need to be delivered during user authorization, you are advised to disable the re-authentication function or set a longer re-authentication interval to improve the device's processing performance.

In remote authentication and authorization, if the re-authentication interval is set to a shorter time, the CPU usage may be higher.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

- Configuring single-time re-authentication
  a. Run **system-view**

     The system view is displayed.
  b. Run **dot1x reauthenticate mac-address** *mac-address*

     The device is manually configured to re-authenticate a user with a specified MAC address once.

**----End**

### 3.6.2.1.7 (Optional) Configuring the Online User Handshake Function

## Context

When a user goes offline due to causes such as network interruption, the device still reserves the user's online information. This may result in incorrect accounting, and brings security threats if a bogus user accesses the network.

To ensure that user online information is normal, you can configure handshake with online 802.1X authentication users on the device. The device then periodically sends handshake request packets to online 802.1X users. If a user does not respond to the handshake request packets when the retransmission count is reached, the device sets the user status to offline.

NOTE

If the 802.1X client cannot exchange handshake packets with the device, the device will not receive the handshake response packets within the handshake period. Therefore, to prevent the device from disconnecting users incorrectly, disable the online user handshake function.

This function takes effect only for the wired users.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **dot1x-access-profile name** *access-profile-name*

The 802.1X access profile view is displayed.

**Step 3** Run **dot1x handshake**

Handshake with online 802.1X authentication users is enabled.

 Copyright © Huawei Technologies Co., Ltd. 

By default, handshake with online 802.1X authentication users is disabled on the device.

**Step 4** (Optional) Run **dot1x timer handshake-period** *handshake-period-value*

The interval at which the device handshakes with 802.1X online users on non-Eth-Trunk interfaces is set.

By default, the interval for sending handshake packets is 15 seconds.

**Step 5** (Optional) Run **dot1x retry** *max-retry-value*

The number of times for resending a handshake packet is configured.

By default, a handshake packet can be resent twice.

**----End**

### 3.6.2.1.8 (Optional) Configuring Network Access Rights for Users When the 802.1X Client Does Not Respond

## Context

If the 802.1X client does not respond, users cannot pass authentication and thereby have no network access right. Before being successfully authenticated, some users may need certain basic network access rights to download client software and update the antivirus database. The network access rights can be configured for the users when the 802.1X client does not respond, so that the users can access specified network resources.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Configure authorization parameters.

- VLAN

  Configure a VLAN and network resources in the VLAN on the device.
- Service scheme

  Configure a service scheme on the device. For configuration details, see **(Optional) Configuring a Service Scheme**.
- User group

  a. Run **user-group** *group-name* [ **group-index** *group-index* ]

  A user group is created and the user group view is displayed.

  b. Run **acl-id** *acl-number*

  An ACL is bound to the user group.

  By default, no ACL is bound to a user group.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

- Before running this command, ensure that an ACL has been created using the **acl (system view)** or **acl name** command and ACL rules have been configured using the **rule** command.
- If a user group contains online users, the ACL bound to the user group cannot be modified or deleted in the system view.

c. Run **user-vlan** *vlan-id*

A user group VLAN is configured.

By default, no user group VLAN is configured.

NOTE

Before running this command, ensure that a VLAN has been created using the **vlan** command.

d. Run **remark** { **8021p** *8021p-value* | **dscp** *dscp-value* | **exp** *exp-value* | **lp** *lp-value* } *

The user group priority is configured.

By default, no user group priority is configured.

e. Run **quit**

Return to the system view.

**Step 3** Run **dot1x-access-profile name** *access-profile-name*

The 802.1X access profile view is displayed.

**Step 4** Run **authentication event client-no-response action authorize** { **service-scheme** *service-scheme-name* | **user-group** *user-group-name* | **vlan** *vlan-id* }

Network access rights are configured for users when the 802.1X client does not respond.

By default, no network access right is configured for users when the 802.1X client does not respond.

**----End**

### 3.6.2.1.9 (Optional) Configuring the Device to Automatically Generate the DHCP Snooping Binding Table for Static IP Users

## Context

There are unauthorized users who modify their MAC addresses to those of authorized users. After authorized users are connected through 802.1X authentication, the unauthorized users can obtain the same identities as the authorized users and connect to the network without authentication. This results in security risks of authentication and accounting. After accessing the network, unauthorized users can also initiate ARP spoofing attacks by sending bogus ARP packets. In this case, the device records incorrect ARP entries, greatly affecting normal communication between authorized users. To prevent the previous attacks, configure IPSG and DAI. These two functions are implemented based on binding tables. For static IP users, you can run the **user-bind static** command to configure

the static binding table. However, if there are many static IP users, it takes more time to configure static binding entries one by one.

To reduce the workload, you can configure the device to automatically generate the DHCP snooping binding table for static IP users. After the static IP users who pass 802.1X authentication or are at the pre-authentication phase send EAP packets to trigger generation of the user information table, the device automatically generates the DHCP snooping binding table based on the MAC address, IP address, and interface recorded in the table.

To make this function take effect, you must run the **dhcp snooping enable** command on the interface to which the 802.1X access profile is bound to enable the DHCP snooping function on the interface and globally.

NOTE

- The EAP protocol does not specify a standard attribute to carry IP address information. Therefore, if the EAP request packet sent by a static IP user does not contain an IP address, the IP address information in the DHCP snooping binding table is obtained from the user' first ARP request packet with the same MAC address as the user information table after the user passes authentication. On a network, unauthorized users may forge authorized users' MAC addresses to initiate ARP snooping attacks to devices, and the DHCP snooping binding table generated accordingly may be unreliable. Therefore, the **dot1x trigger dhcp-binding** command is not recommended and you are advised to run the **user-bind static** command to configure the static binding table.
- For users who are assigned IP addresses using DHCP, you do not need to run the **dot1x trigger dhcp-binding** command on the device. The DHCP snooping binding table is generated through the DHCP snooping function.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **dot1x-access-profile name** *access-profile-name*

The 802.1X access profile view is displayed.

**Step 3** Run **dot1x trigger dhcp-binding**

The device is configured to automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-authentication phase.

By default, the device does not automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-authentication phase.

**----End**

## Verifying the Configuration

You can run the **display dhcp snooping user-bind** command to check the DHCP snooping binding table that is generated by the device for static IP users who pass 802.1X authentication or are at the pre-authentication phase. The DHCP snooping binding table generated using this function will be deleted after the users are disconnected.

 Copyright © Huawei Technologies Co., Ltd. 

## Follow-up Procedure

Configure IPSG and DAI after the DHCP snooping binding table is generated, prevent attacks from unauthorized users.

- In the interface view, run the **ip source check user-bind enable** command to enable IPSG.
- In the interface view, run the **arp anti-attack check user-bind enable** command to enable DAI.

For detailed configurations of IPSG and DAI, see **IPSG Configuration** and **ARP Security Configuration** in the *Huawei AR Series V200R010 Configuration Guide - Security*.

### 3.6.2.1.10 (Optional) Configuring the Number of Times an Authentication Request or Handshake Packet Is Retransmitted to an 802.1X User

## Context

If the device does not receive any response from a user within a specified time after sending an authentication request or handshake packet to the user, the device sends the authentication request or handshake packet again. If the authentication request or handshake packet has been sent for the maximum retransmission times and no response is received, the user authentication or handshake fails. In this process, the total number of authentication requests or handshake packets sent by the device is *max-retry-value* plus 1.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **dot1x-access-profile name** *access-profile-name*

The 802.1X access profile view is displayed.

**Step 3** Run **dot1x retry** *max-retry-value*

The number of times an authentication request or handshake packet is retransmitted to an 802.1X client is configured.

By default, the device can retransmit an authentication request or handshake packet to an 802.1X user twice.

**----End**

### 3.6.2.1.11 (Optional) Configuring the Authentication Timeout Timer for 802.1X Clients

## Context

The device starts the authentication timeout timer for 802.1X clients after sending an EAP-Request/MD5-Challenge packet to a client. If the client does not respond within the period set by this timer, the device sends the packet again. If the packet has been sent for the maximum number of times (configured using the **dot1x**

 Copyright © Huawei Technologies Co., Ltd. 

**retry** *max-retry-value* command) and no response is received, the device stops sending the packet. This prevents repeated retransmission of authentication requests, which occupies lots of resources.

Generally, if the client fails to be authenticated, the device starts a backup mechanism (MAC address authentication, Portal authentication, or granting specified access permission), so that the client can continue to access the network. The value of the timeout timer for EAP-Request/MD5 Challenge packets is calculated as follows:

Timer value = (*max-retry-value* + 1) x *client-timeout-value*

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **dot1x-access-profile name** *access-profile-name*

The 802.1X access profile view is displayed.

**Step 3** Run **dot1x timer client-timeout** *client-timeout-value*

The authentication timeout timer for 802.1X clients is configured.

By default, the authentication timeout timer for 802.1X clients is enabled and its value is 5 seconds.

**Step 4** (Optional) Run **dot1x retry** *max-retry-value*

The number of times an authentication request is retransmitted to an 802.1X client is configured.

By default, the device can retransmit an authentication request to an 802.1X user twice.

**----End**

### 3.6.2.1.12 (Optional) Configuring the Function of Triggering 802.1X Authentication Through Multicast Packets

## Context

If clients such as the built-in 802.1X client on the Windows operating system cannot send EAPoL-Start packets for 802.1X authentication, you can configure the function of triggering 802.1X authentication through multicast packets on the device. The device then periodically multicasts EAP-Request/Identity packets to clients to trigger 802.1X authentication for the clients.

If the device interface connecting to a client changes from Down to Up, the client needs to send EAPoL-Start packets again for 802.1X authentication, which takes a long time. You can enable the function of triggering 802.1X authentication through multicast packets immediately after the device interface goes Up, shortening the re-authentication time.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **dot1x mc-trigger**

The function of triggering 802.1X authentication through multicast packets is enabled.

By default, the function of triggering 802.1X authentication through multicast packets is enabled.

**Step 3** (Optional) Run **dot1x mc-trigger port-up-send enable**

The function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up is enabled.

By default, the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up is disabled.

**----End**

### 3.6.2.1.13 (Optional) Configuring MAC Address-based Dynamic VLAN Assignment

## Context

After you run the **dynamic-macvlan enable** command on a port and 802.1X or MAC address authentication is completed, the VLAN attribute assigned by the RADIUS server is added to the packets sent to the CPU regardless of the port from which users access the network. In this manner, a MAC address-to-VLAN mapping is created and packets are not directed based on the PVID.

NOTE

Only the AR1220E, AR1220EV, AR1220EVW, and AR1220F support this function.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface gigabitethernet** *interface-number*

The GE interface view is displayed.

**Step 3** Run **dynamic-macvlan enable**

MAC address-based dynamic VLAN assignment is enabled.

By default, MAC address-based dynamic VLAN assignment is disabled.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

- This command can be run only on Layer 2 ports of the device panel.
- The ports must be of the hybrid untagged type.
- The ports enabled with MAC address-based dynamic VLAN assignment support Layer 3 services only.
- If a port has an authentication profile applied, you need to unbind the authentication profile from the port before running the **dynamic-macvlan enable** command.

**----End**

#### 3.6.2.1.14 Verifying the 802.1X Access Profile Configuration

### Context

After configuring an 802.1X access profile, run the following command to check the configuration.

### Procedure

- Run the **display dot1x-access-profile configuration** [ **name** *access-profile-name* ] command to check the configuration of the 802.1X access profile.

**----End**

### 3.6.2.2 Configuring a MAC Access Profile

#### 3.6.2.2.1 Creating a MAC Access Profile

### Context

The device uses MAC access profiles to uniformly manage MAC users access configurations. Before configuring MAC address authentication, you need to create a MAC access profile.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **mac-access-profile name** *access-profile-name*

A MAC access profile is created and the MAC access profile view is displayed.

By default, the device has the built-in MAC access profile **mac_access_profile**.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

- The device supports a maximum of 8 configurable MAC access profiles. The compatibility profile converted after an upgrade is not counted in the configuration specification. The built-in MAC access profile **mac_access_profile** can be modified and applied, but cannot be deleted.
- Before deleting a MAC access profile, ensure that this profile is not bound to any authentication profile.

**----End**

### 3.6.2.2.2 (Optional) Configuring the Authentication Mode for MAC Address Authentication

## Context

In MAC address authentication, the access device exchanges RADIUS packets with the authentication server. Differences between authentication modes PAP and CHAP are as follows:

- PAP is a two-way handshake authentication protocol. It transmits passwords in plain text format in RADIUS packets.
- CHAP is a three-way handshake authentication protocol. It transmits only user names but not passwords in RADIUS packets. CHAP is more secure and reliable than PAP. If high security is required, CHAP is recommended.

By default, the authentication mode for MAC address authentication is set to PAP. The authentication mode can be changed to CHAP for higher security.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **mac-access-profile name** *access-profile-name*

The MAC access profile view is displayed.

**Step 3** Run **mac-authen authentication-method** { **chap** | **pap** }

The authentication mode for MAC address authentication is configured.

By default, the authentication mode is set to PAP.

**----End**

### 3.6.2.2.3 Configuring the User Name Format for MAC Address Authentication

## Context

The following user name formats are available for MAC address authentication:

- MAC address: A user uses the MAC address as the user name for authentication, and uses the MAC address or a user-defined character string as the password.

 Copyright © Huawei Technologies Co., Ltd. 

- Fixed user name: All users use a fixed name and password configured on the device for authentication, regardless of their MAC addresses. Only one user account needs to be configured on the authentication server. This method can be used on a network where access clients are reliable.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **mac-access-profile name** *access-profile-name*

The MAC access profile view is displayed.

**Step 3** Run **mac-authen username** { **fixed** *username* [ **password cipher** *password* ] | **macaddress** [ **format** { **with-hyphen** [ **normal** ] [ **colon** ] | **without-hyphen** } [ **uppercase** ] [ **password cipher** *password* ] ] }

The user name format is configured for MAC address authentication.

By default, a MAC address without hyphens (-) or colons (:) is used as the user name and password for MAC address authentication.

NOTE

- When configuring the user name format for MAC address authentication, ensure that the authentication server supports the user name format.
- If MAC address authentication is enabled on a WLAN-ESS interface, passwords must be configured.

**----End**

### 3.6.2.2.4 (Optional) Configuring Packet Types That Can Trigger MAC Address Authentication

## Context

After MAC address authentication is enabled, the device can trigger MAC address authentication on users by default when receiving DHCP/ARP packets. Based on user information on the actual network, the administrator can adjust the packet types that can trigger MAC address authentication. For example, if all users on a network dynamically obtain IPv4 addresses, the device can be configured to trigger MAC address authentication only through DHCP packets. This prevents the device from continuously sending ARP packets to trigger MAC address authentication when static IPv4 addresses are configured for unauthorized users on the network, and reduces device CPU occupation.

When the function of triggering MAC address authentication through DHCP packets is supported, the device can use the DHCP packets to re-authenticate users, clear the MAC address authentication user entries in time, and send user terminal information to the authentication server.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

- After the VLANIF interface is enabled with the MAC address authentication function, MAC address authentication cannot be triggered for users when the interface receives DHCP packets.
- This function takes effect only for users who go online after this function is successfully configured.
- Only wired users support MAC address authentication triggered by DHCP/ARP packets. For wireless users, MAC address authentication is triggered by association packets.
- When MAC address authentication and 802.1X authentication are both enabled on an interface, packets that can trigger authentication include all the packet types that can trigger authentication in the MAC access profile and 802.1X access profile. For example, assume that ARP packets in the MAC access profile are unable to trigger authentication and ARP packets in the 802.1X access profile can trigger authentication. If MAC address authentication and 802.1X authentication are both enabled on an interface, ARP packets can trigger MAC address authentication.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **mac-access-profile name** *access-profile-name*

The MAC access profile view is displayed.

**Step 3** Run **authentication trigger-condition** { **dhcp** | **arp** } *

The packet types that can trigger MAC address authentication are configured.

By default, DHCP/ARP packets can trigger MAC address authentication.

**----End**

### 3.6.2.2.5 (Optional) Configuring a Source MAC Address Segment Allowed by MAC Address Authentication

## Context

After MAC address authentication is enabled, MAC address authentication will be performed for every new MAC address entry generated on the device. To restrict the users for whom MAC address authentication can be performed on interfaces, you can configure a source MAC address segment allowed by MAC address authentication.

NOTE

Only MAC address authentication users who go online through VLANIF interfaces support this function.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 2** Run **mac-access-profile name** *access-profile-name*

The MAC access profile view is displayed.

**Step 3** Run **mac-authen permit mac-address** *mac-address* **mask** { *mask* | *mask-length* }

The source MAC address segment allowed by MAC address authentication is configured.

By default, no source MAC address segment is configured for MAC address authentication.

**----End**

### 3.6.2.2.6 (Optional) Configuring Re-authentication for Online MAC Address Authentication Users

## Context

If the administrator modifies parameters such as access rights and authorization attributes of an online user on the authentication server, the user must be re-authenticated to ensure user validity.

If re-authentication is configured for online MAC address authentication users, the device sends saved authentication parameters of an online user to the authentication server for re-authentication. The device saves user authentication information after users go online. If the user authentication information on the authentication server remains unchanged, the user keeps online. If the information has been modified, the user is disconnected and needs to be re-authenticated.

The device re-authenticates MAC address authentication users in the following modes:

- The device periodically re-authenticates users using a specified MAC access profile.

  NOTE

  After this function is configured, many MAC address authentication logs will be generated.
- The device re-authenticates MAC address authentication users when receiving DHCP lease renewal packets from the users. This mode takes effect only after the device is configured to trigger MAC address authentication through DHCP packets.
- The device is manually configured to re-authenticate a user with a specified MAC address once.

## Procedure

- Configuring periodic re-authentication
  a. Run **system-view**

     The system view is displayed.
  b. Run **mac-access-profile name** *access-profile-name*

     The MAC access profile view is displayed.
  c. Run **mac-authen reauthenticate**

 Copyright © Huawei Technologies Co., Ltd. 

Re-authentication is enabled for online MAC address authentication users.

By default, re-authentication for online MAC address authentication users is disabled.

d. (Optional) Run **mac-authen timer reauthenticate-period** *reauthenticate-period-value*

The re-authentication interval is configured for online MAC address authentication users.

By default, the re-authentication interval is 1800 seconds for online MAC address authentication users.

NOTE

It is recommended that the re-authentication interval be set to the default value. If multiple ACLs need to be delivered during user authorization, you are advised to disable the re-authentication function or set a longer re-authentication interval to improve the device's processing performance.

In remote authentication and authorization, if the re-authentication interval is set to a shorter time, the CPU usage may be higher.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

- Configuring single-time re-authentication
  a. Run **system-view**

  The system view is displayed.

  b. Run **mac-authen reauthenticate mac-address** *mac-address*

  The device is manually configured to re-authenticate a user with a specified MAC address once.

**----End**

### 3.6.2.2.7 (Optional) Configuring the Device to Automatically Generate the DHCP Snooping Binding Table for Static IP Users

## Context

There are unauthorized users who modify their MAC addresses to those of authorized users. After authorized users are connected through MAC address authentication, the unauthorized users can obtain the same identities as the authorized users. This results in security risks of authentication and accounting. After accessing the network, unauthorized users can also initiate ARP spoofing attacks by sending bogus ARP packets. In this case, the device records incorrect ARP entries, greatly affecting normal communication between authorized users. To prevent the previous attacks, configure IPSG. This function is implemented based on binding tables. For static IP users, you can run the **user-bind static** command to configure the static binding table. However, if there are many static IP users, it takes more time to configure static binding entries one by one.

To reduce the workload, you can configure the device to automatically generate the DHCP snooping binding table for static IP users. After this function is enabled, the device automatically generates the DHCP snooping binding table based on the

 Copyright © Huawei Technologies Co., Ltd. 

MAC address, IP address, and interface information of static IP users who pass MAC address authentication or are at the pre-authentication phase.

NOTE

For users who are assigned IP addresses using DHCP, you do not need to run the **mac-authen trigger dhcp-binding** command on the device. The DHCP snooping binding table is generated through the DHCP snooping function.

## Prerequisites

To make this function take effect, you must run the **dhcp snooping enable** command on the interface to which the mac access profile is bound to enable the DHCP snooping function on the interface and globally.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **mac-access-profile name** *access-profile-name*

The MAC access profile view is displayed.

**Step 3** Run **mac-authen trigger dhcp-binding**

The device is configured to automatically generate the DHCP snooping binding table after static IP users pass MAC address authentication or when the users are at the pre-authentication phase.

By default, the device does not automatically generate the DHCP snooping binding table after static IP users pass MAC address authentication or when the users are at the pre-authentication phase.

**----End**

## Verifying the Configuration

You can run the **display dhcp snooping user-bind** command to check the DHCP snooping binding table that is generated by the device for static IP users who pass MAC address authentication or are at the pre-authentication phase. The DHCP snooping binding table generated using this function will be deleted after the users are disconnected.

## Follow-up Procedure

Configure IPSG and DAI after the DHCP snooping binding table is generated, prevent attacks from unauthorized users.

- In the interface view, run the **ip source check user-bind enable** command to enable IPSG.

For detailed configuration of IPSG, see **IPSG Configuration** in the *Huawei AR Series V200R010 Configuration Guide - Security*.

 Copyright © Huawei Technologies Co., Ltd. 

#### 3.6.2.2.8 (Optional) Configuring MAC Address-based Dynamic VLAN Assignment

### Context

After you run the **dynamic-macvlan enable** command on a port and 802.1X or MAC address authentication is completed, the VLAN attribute assigned by the RADIUS server is added to the packets sent to the CPU regardless of the port from which users access the network. In this manner, a MAC address-to-VLAN mapping is created and packets are not directed based on the PVID.

NOTE

Only the AR1220E, AR1220EV, AR1220EVW, and AR1220F support this function.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface gigabitethernet** *interface-number*

The GE interface view is displayed.

**Step 3** Run **dynamic-macvlan enable**

MAC address-based dynamic VLAN assignment is enabled.

By default, MAC address-based dynamic VLAN assignment is disabled.

NOTE

- This command can be run only on Layer 2 ports of the device panel.
- The ports must be of the hybrid untagged type.
- The ports enabled with MAC address-based dynamic VLAN assignment support Layer 3 services only.
- If a port has an authentication profile applied, you need to unbind the authentication profile from the port before running the **dynamic-macvlan enable** command.

**----End**

#### 3.6.2.2.9 Verifying the MAC Access Profile Configuration

### Context

After configuring a MAC access profile, run the following command to check the configuration.

### Procedure

- Run the **display mac-access-profile configuration** [ **name** *access-profile-name* ] command to check the configuration of the MAC access profile.

**----End**

## 3.6.3 Configuring an Authentication Profile

 Copyright © Huawei Technologies Co., Ltd. 

### 3.6.3.1 Creating an Authentication Profile

## Context

NAC implements access control on users. To facilitate NAC function configuration, the device uses authentication profiles to uniformly manage NAC configuration. You can configure parameters in an authentication profile to provide different access control modes for users. For example, you can configure the access profile bound to the authentication profile to determine the authentication mode for the authentication profile. The device then uses the authentication mode to authenticate users on the interface or VAP profile to which the authentication profile is applied.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **authentication-profile name** *authentication-profile-name*

An authentication profile is created and the authentication profile view is displayed.

By default, the device has six built-in authentication profiles: default_authen_profile, dot1x_authen_profile, mac_authen_profile, portal_authen_profile, dot1xmac_authen_profile, and multi_authen_profile.

NOTE

- The device supports a maximum of 8 authentication profiles. The built-in authentication profile **default_authen_profile** and the compatibility profile converted after an upgrade are not counted in the configuration specification. The six built-in authentication profiles (default_authen_profile, dot1x_authen_profile, mac_authen_profile, portal_authen_profile, dot1xmac_authen_profile, and multi_authen_profile) can be modified and applied, but cannot be deleted.
- Before deleting an authentication profile, ensure that this profile is not bound to any interface or VAP profile. You can run the **display authentication-profile configuration** command to check whether the authentication profile is bound to interface or VAP profile

**----End**

### 3.6.3.2 Configuring a User Authentication Mode

## Context

The device supports 802.1X, MAC address modes in NAC deployment. The access profile bound to the authentication profile determines the user authentication mode in a VAP profile. For example, if you want to use MAC address authentication to control and manage users who go online using a VAP profile, bind a MAC access profile to the authentication profile applied to the VAP profile.

The device allows multiple authentication modes (multi-mode authentication) to be deployed simultaneously in a VAP profile to meet various authentication requirements on the network. In this case, you need to bind multiple access profiles to an authentication profile.

 Copyright © Huawei Technologies Co., Ltd. 

## Prerequisites

Access profiles have been configured.

- For details about how to configure an 802.1X access profile, see **3.6.2.1 Configuring an 802.1X Access Profile**.
- For details about how to configure a MAC access profile, see **3.6.2.2 Configuring a MAC Access Profile**.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **authentication-profile name** *authentication-profile-name*

The authentication profile view is displayed.

**Step 3** Configure the user authentication mode.

- 802.1X authentication

  Run **dot1x-access-profile** *access-profile-name*

  An 802.1X access profile is bound to the authentication profile.

  By default, no 802.1X access profile is bound to an authentication profile.
- MAC address authentication

  Run **mac-access-profile** *access-profile-name*

  A MAC access profile is bound to the authentication profile.

  By default, no MAC access profile is bound to an authentication profile.
- Portal authentication

  Run **portal-access-profile** *access-profile-name*

  A Portal access profile is bound to the authentication profile.

  By default, no Portal access profile is bound to an authentication profile.

  NOTE

  For wireless users, the Portal access profile template can be bound to only the VLANIF interface.
- Multi-mode authentication

  To concurrently configure several authentication modes, you only need to bind corresponding access profiles to an authentication profile. Access profiles can be bound to the authentication profile in any sequence. The device triggers the corresponding authentication based on received authentication packets.

  You can configure MAC address bypass authentication to authenticate terminals such as printers that cannot have the 802.1X client installed. The device performs 802.1X authentication for users. If the authentication fails, the device performs MAC address authentication for these users.

  The following uses MAC address bypass authentication as an example. The configuration procedure is as follows:

  a. Run **mac-access-profile** *access-profile-name*

 Copyright © Huawei Technologies Co., Ltd. 

A MAC access profile is bound to the authentication profile.

By default, no MAC access profile is bound to an authentication profile.

b. Run **dot1x-access-profile** *access-profile-name*

An 802.1X access profile is bound to the authentication profile.

By default, no 802.1X access profile is bound to an authentication profile.

c. Run **authentication dot1x-mac-bypass**

MAC address bypass authentication is enabled.

By default, MAC address bypass authentication is disabled.

NOTE

When configuring multi-mode authentication, pay attention to the following points:

- An authentication profile can be bounded to an 802.1X access profile, a MAC access profile and a Portal access profile at most.
- After multi-mode authentication is configured, the device by default allows users to use multiple authentication modes. For example, if a user passes MAC address authentication, the user will not be redirected to the Portal authentication page when accessing a web page. However, if the user directly enters the Portal authentication website in the browser, Portal authentication can be performed. After the authentication succeeds, the users can obtain network access rights for Portal authentication users. To authenticate users using only one authentication mode, run the **authentication single-access** command to configure the device to allow users to pass only one access authentication.

**Step 4** (Optional) Run **authentication ip-address in-accounting-start**

The function of carrying users' IP addresses in Accounting-Start packets is enabled.

By default, the function of carrying users' IP addresses in Accounting-Start packets is disabled.

This command takes effect only for 802.1X authentication and MAC address authentication users. By default, Accounting-Start packets for Portal authentication carry users' IP addresses.

**Step 5** (Optional) Run **authentication roam pre-authen mac-authen enable**

MAC address authentication is enabled for roaming STAs.

By default, MAC address authentication is disabled for roaming STAs.

**----End**

## 3.6.3.3 (Optional) Configuring the User Access Mode

## Context

After enabling NAC authentication, you can configure a user access mode based on the user access on the interface. The user access modes include:

- **single-terminal**: applies to the scenario in which only one data terminal is connected to the network through the interface.
- **single-voice-with-data**: applies to the scenario in which only one data terminal is connected to the network on the device interface through a voice terminal.

 Copyright © Huawei Technologies Co., Ltd. 

- **multi-share**: applies to the scenario that does not require high security and in which multiple data terminals are connected to the network on the device interface.
- **multi-authen**: applies to the scenario that requires high security and in which multiple data terminals are connected to the network on the device interface. In this access mode, you can configure the maximum number of access users based on the actual user quantity on the interface. This prevents malicious users from occupying a large amount of device resources and ensures that the users on other device interfaces can normally go online.

NOTE

AR100&AR120&AR150&AR160&AR200&AR1200 series do not support to bind a VLAN in MAC-based mode.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **authentication-profile name** *authentication-profile-name*

The authentication profile view is displayed.

**Step 3** Run **authentication mode** { **single-terminal** | **single-voice-with-data** | **multi-share** | **multi-authen** [ **max-user** *max-user-number* [ **dot1x** | **mac-authen** | **portal** | **none** ] * ] }

The maximum number of access users allowed on the interface is configured when the user access mode or interface access authentication mode is **multi-authen**.

By default, the access authentication mode is **multi-authen**.

NOTE

- VLANIF interfaces do not support this function.
- Only wired users support this function.
- If the first access user fails to be authenticated on a physical interface and sets up a pre-connection after the **multi-share** mode is configured on the physical interface, new access users will also fail to be authenticated on the interface. Therefore, the following operations are recommended if the first access user may fail to be authenticated after the **multi-share** mode is configured on a physical interface.
  - Do not use the **multi-share** mode with Portal authentication.

**----End**

## 3.6.3.4 (Optional) Configuring Authentication Event Authorization Information

## Context

If users establish pre-connections with the device or fail to be authenticated, they have no network access rights.

 Copyright © Huawei Technologies Co., Ltd. 

To meet these users' basic network access requirements such as updating the antivirus database and downloading the client, configure authentication event authorization information. The device will assign network access rights to these users based on the authentication phase.

NOTE

An authorized VLAN cannot be delivered to online Portal users.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Configure authorization parameters.

If users are in the pre-connection phase or fail to be authenticated, or the authentication server is Down, the device can use the VLAN and service scheme to grant network access rights to the users.

- VLAN

  Configure a VLAN and network resources in the VLAN on the device.
- Service scheme

  Configure a service scheme on the device. For configuration details, see **(Optional) Configuring a Service Scheme**.

**Step 3** Run **authentication-profile name** *authentication-profile-name*

The authentication profile view is displayed.

**Step 4** Configure authorization information.

- Run **authentication event pre-authen action authorize** { **vlan** *vlan-id* | **service-scheme** *service-scheme-name* }

  Network access rights are configured for users who are in the pre-connection phase.
- Run **authentication event authen-fail action authorize** { **vlan** *vlan-id* | **service-scheme** *service-scheme-name* } [ **response-fail** ]

  Network access rights are configured for users who fail to be authenticated.
- Run **authentication event authen-server-down action authorize** { **vlan** *vlan-id* | **service-scheme** *service-scheme-name* } [ **response-fail** ]

  Network access rights are configured for users when the authentication server is Down.

By default, no authentication event authorization information is configured.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

If no network access right is configured for users who fail authentication or when the authentication server is Down, the users establish pre-connections with the device after the authentication fails and then have the network access rights mapping pre-connection users.

Only the 8FE1GE, 24GE, and 24ES2GP cards, and the AR2201-48FE and AR2202-48FE support the delivery of authorized VLANs to users.

VLAN-based authorization does not apply to the authentication users who access through VLANIF interfaces.

In 802.1X authentication for wired users, when the RADIUS server is Down, some new clients do not have escape rights. For example, when a new Windows client receives a Success packet from the device but does not receive the authentication packets exchanged with the RADIUS server, the client will fail the authentication and cannot go online. Currently, the following clients have escape rights when they go online for the first time: H3C iNode clients using EAP-MD5 or PEAP and Cisco AnyConnect clients using EAP-FAST or PEAP. For Windows clients, for example, Windows 7, choose "Local Area Connection> Properties> Authentication> Fallback to unauthorized network access".

If authorization upon an authentication server Down event is configured and the device detects that the authentication server is Down, the device grants corresponding network access rights to users who fail to be authenticated, and add the users to entries of users who fail to be authenticated upon an authentication server Down event. If authorization upon an authentication server Down event is not configured and the device detects that the authentication server is Down, the device grants corresponding network access rights to users who fail to be authenticated, and add the users to entries of users who fail to be authenticated.

The device assigns network access rights based on the priorities of the configured rights in a network status as follows:

- If the authentication server is Down: network access right upon an authentication server Down event > network access right for users who fail authentication > network access right for users in the pre-connection state > user authorization based on whether the function of keeping users who fail to be authenticated and do not have any network access rights in the pre-connection state is enabled
- If users fail authentication: network access right for users who fail authentication > network access right for users in the pre-connection state > user authorization based on whether the function of keeping users who fail to be authenticated and do not have any network access rights in the pre-connection state is enabled
- If users are in the pre-connection state: network access right for users in the pre-connection state > user authorization based on whether the function of keeping users who fail to be authenticated and do not have any network access rights in the pre-connection state is enabled
- If an 802.1X client does not respond: network access right if an 802.1X client does not respond > network access right for users in the pre-connection state > user authorization based on whether the function of keeping users who fail to be authenticated and do not have any network access rights in the pre-connection state is enabled

**Step 5** (Optional) Configure the aging time of user entries.

- Run **authentication timer pre-authen-aging** *aging-time*

  The aging time is configured for entries of pre-connection users.

  By default, the aging time is 23 hours for entries of pre-connection users.

- Run **authentication timer authen-fail-aging** *aging-time*

  The aging time is configured for entries of users who fail to be authenticated.

  By default, the aging time is 23 hours for entries of users who fail to be authenticated.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

You can run the **authentication timer authen-fail-aging** *aging-time* command to configure the aging time for entries of users who fail to be authenticated upon an authentication server Down event and entries of users who fail to be authenticated.

**----End**

## 3.6.3.5 (Optional) Configuring Authentication-Free Authorization Information

### 3.6.3.5.1 (Optional) Configuring Authorization Information for Authentication-free Users

## Context

Before being authenticated, users need to obtain some network access rights to meet basic network access requirements such as downloading the 802.1X client and updating antivirus database. The device uses an authentication-free rule profile to uniformly manage authorization information for authentication-free users. You can define some network access rules in the profile to determine network access rights that can be obtained by authentication-free users. You need to bind a configured authentication-free rule profile to an authentication profile. Users using the authentication profile then can obtain authentication-free authorization information.

NOTE

Authentication-free rules can take effect immediately after being configured in an authentication-free profile. It is unnecessary to bind the authentication-free profile to an authentication profile.

## Procedure

**Step 1** Configure an authentication-free rule profile.

1. Run **system-view**

   The system view is displayed.

2. Run **free-rule-template name** *free-rule-template-name*

   An authentication-free rule profile is created and the authentication-free rule profile view is displayed.

   By default, the device has a built-in authentication-free rule profile named default_free_rule.

   NOTE

   Currently, the device supports only one authentication-free rule profile, that is, the built-in profile **default_free_rule**.

3. Run **free-rule** *rule-id* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } } | **source** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } } } *

   Or run **free-rule acl** *acl-id*

   An authentication-free rule is configured.

 Copyright © Huawei Technologies Co., Ltd. 

By default, no authentication-free rule is configured for NAC authentication users.

4. Run **quit**

   Return to the system view.

**Step 2** Bind the authentication-free rule profile to the authentication profile.

1. Run **authentication-profile name** *authentication-profile-name*

   The authentication profile view is displayed.

2. Run **free-rule-template** *free-rule-template-name*

   Bind the authentication-free rule profile to the authentication profile.

   By default, no authentication-free rule profile is bound to an authentication profile.

**----End**

## 3.6.3.6 (Optional) Configuring Re-authentication for Users

### Context

The device records entries for pre-connection users and users who fail to be authenticated, and grants corresponding network access rights to the users. For details, see **3.6.3.4 (Optional) Configuring Authentication Event Authorization Information**. To ensure that users are successfully authenticated in a timely manner and obtain normal network access rights, you can configure the device to re-authenticate users who fail to be authenticated based on user entries.

If a user fails to be re-authenticated before the aging time expires, the device deletes the corresponding user entry and reclaims the granted network access rights. If a user is successfully re-authenticated, the device adds the user to entries of authenticated users and grants corresponding network access rights to the user.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **authentication-profile name** *authentication-profile-name*

The authentication profile view is displayed.

**Step 3** Run **authentication timer re-authen** { **pre-authen** *re-authen-time* | **authen-fail** *re-authen-time* }

A re-authentication interval is configured for pre-connection users and users who fail to be authenticated.

By default, the device re-authenticates pre-connection users and users who fail to be authenticated at an interval of 60 seconds.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

The device adds users with the **authen-fail** authorization and pre-connection users to entries of users who fail to be authenticated or pre-connection users. By default, the device re-authenticates users in the entries. You can perform the preceding operations to change the re-authentication interval.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

**Step 4** Run **authentication event authen-server-up action re-authen**

The device is enabled to re-authenticate users in the survival state when the authentication server changes from Down or forcible Up to Up.

By default, the device does not re-authenticate users in the survival state when the authentication server changes from Down or forcible Up to UP.

NOTE

After the status of the RADIUS server is set to Down, you can run the **radius-server dead-time** *dead-time* command to set the interval for the RADIUS server to return to the active state. When the value of *dead-time* expires, the status of the RADIUS server is set to forcible Up. When the server successfully transmits and receives packets, the status is set to Up. The device can re-authenticate users when the server changes from Down or forcible Up to Up.

**----End**

## 3.6.3.7 (Optional) Configuring the Handshake Function to Enable the Device to Clear User Entries Immediately

## Context

The device creates entries for pre-connection users, users who fail to be authenticated and are assigned network access rights, and users who are authenticated. After users go offline in normal situations, the system immediately deletes the corresponding user entries. However, if some users go offline due to exceptions such as network disconnections, the system cannot immediately delete the corresponding user entries. If there are too many such invalid user entries, other users may fail to access the network.

To solve this problem, configure the handshake function to enable the device to clear user entries immediately. Then, if a user does not respond to the handshake request from the device within the handshake interval, the device deletes the user entry.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

All pre-connection users support this function. Among users who fail to be authenticated or pass authentication, only MAC address authentication users, and 802.1X authentication users support this function. The offline detection function for Portal authentication users is configured using the **portal timer offline-detect** command.

This function takes effect only for the wired users who obtain IP addresses.

If the number of ARP probe packets exceeds the default CAR value, the probe fails and the users are logged out (The **display cpu-defend statistics** command can be run to check whether ARP request and response packets are lost.). To resolve the problem, the following methods are recommended:

- Increase the handshake interval based on the number of users. The default handshake interval is recommended when there are less than 8000 users; the handshake interval should be no less than 600 seconds when there are more than 8000 users.
- Deploy the port attack defense function on the access device and limit the rate of packets sent to the CPU.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **authentication-profile name** *authentication-profile-name*

The authentication profile view is displayed.

**Step 3** Run **authentication handshake**

The handshake with pre-connection users and authorized users is enabled.

By default, the handshake with pre-connection users and authorized users is enabled.

**Step 4** (Optional) Run **authentication timer handshake-period** *handshake-period*

The handshake interval of the device with pre-connection users and authorized users is set.

By default, the handshake interval of the device with pre-connection users and authorized users is 300 seconds.

**----End**

## 3.6.3.8 (Optional) Configuring a User Authentication Domain

## Context

The device manages users in domains. For example, AAA schemes and authorization information are bound to domains. During user authentication, the device assigns users to specified domains based on the domain names contained in user names. However, user names entered by many users on actual networks do not contain domain names. In this case, you can configure a default domain in an authentication profile. If users using this profile enter user names that do not contain domain names, the device manages the users in the default domain.

On actual networks, user names entered by some users contain domain names and those entered by other users do not. The device uses different domains to

 Copyright © Huawei Technologies Co., Ltd. 

manage the users. Because authentication, authorization and accounting (AAA) information in the domains are different, users use different AAA information. To ensure that users using the same authentication profile use the same AAA information, you can configure a forcible domain in the authentication profile for the users. The device then manages the users in the forcible domain regardless of whether entered user names contain domain names or not.

## Prerequisites

A domain has been configured using the **domain (AAA view)** command in the AAA view.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **authentication-profile name** *authentication-profile-name*

The authentication profile view is displayed.

**Step 3** Run **access-domain** *domain-name* [ **dot1x** | **mac-authen** | **portal** ] * [ **force** ]

A default or forcible domain is configured for users.

By default, no default or forcible domain is configured in an authentication profile, and the global default domain **default** is used.

NOTE

- If **force** is not specified, a default domain is configured. If **force** is specified, a forcible domain is configured. If both a default domain and a forcible domain are configured, the device authenticates users in the forcible domain.
- If **dot1x**, **mac-authen**, or **portal** is not specified, the configured domain takes effect for all access authentication users using the authentication profile. If **dot1x**, **mac-authen**, or **portal** is specified, the configured domain takes effect only for specified users using the authentication profile.
- To configure the authentication domain for MAC address authentication users, run the **mac-authen domain** *isp-name* **mac-address** *mac-address* **mask** *mask* command in the system view. When **access-domain mac-authen** and **mac-authen domain** are both configured, **access-domain mac-authen**preferentially takes effect.

**----End**

## 3.6.3.9 (Optional) Configuring the User Logout Delay Function When an Interface Link Is Faulty

## Context

If a link is faulty, the interface is interrupted and users are directly logged out. To solve this problem, you can configure the user logout delay function. When the interface link is faulty, the users remain online within the delay. In this case, if the link is restored, the users do not need to be re-authenticated. If the users are disconnected after the delay and the link is restored, the users need to be re-authenticated.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

- This function takes effect only for wired users who go online on Layer 2 physical interfaces that have been configured with NAC authentication.
- To make the function take effect, it is recommended that the configured interval be greater than the time during which the interface is in Up state.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **authentication-profile name** *authentication-profile-name*

The authentication profile view is displayed.

**Step 3** Run **link-down offline delay** { *delay-value* | **unlimited** }

The user logout delay is configured when an interface link is faulty.

The default user logout delay is 10 seconds when an interface link is faulty.

If the delay is 0, users are logged out immediately when the interface link is faulty. If the delay is **unlimited**, users are not logged out when the interface link is faulty.

**----End**

## 3.6.3.10 (Optional) Reauthenticating users When the Time Exceeds the Value of Session-Timeout

## Context

The RADIUS server uses the **Session-Timeout** attribute to control the remaining online time of a user, and uses the **Termination-Action** attribute to determine whether to reauthenticate the user when the timeout interval expires. By default, if the RADIUS server delivers **Session-Timeout** but no **Termination-Action**, the device disconnects users when the time exceeds the value of **Session-Timeout**. To reauthenticate users without modifying the server configuration, you can run this command to configure the device to reauthenticate users when the timeout interval expires.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **authentication-profile name** *authentication-profile-name*

The authentication profile view is displayed.

**Step 3** Run **authentication termination-action reauthenticate**

The device is configured to reauthenticate users when the time exceeds the value of **Session-Timeout** delivered by the RADIUS server.

 Copyright © Huawei Technologies Co., Ltd. 

By default, the device is not configured to reauthenticate users when the time exceeds the value of **Session-Timeout** delivered by the RADIUS server.

**----End**

### 3.6.3.11 Verifying the Authentication Profile Configuration

#### Context

After configuring an authentication profile, run the following commands to verify the configuration.

#### Procedure

- Run the **display authentication-profile configuration** [ **name** *authentication-profile-name* ] command to check the configuration of the authentication profile.
- Run the **display free-rule-template configuration** [ **name** *free-rule-name* ] command to check the configuration of the authentication-free rule profile.

**----End**

## 3.6.4 NAC Application

#### Context

After an authentication profile is bound to the interface or VAP profile, NAC is enabled in the interface or VAP profile. The device implements access control on users who go online through the interface or VAP profile.

An authentication profile uniformly manages NAC configuration. The authentication profile is bound to the interface or VAP profile view to enable NAC, implementing access control on the users in the interface or VAP profile. The authentication type of the users in the interface or VAP profile is determined by the access profile bound to the authentication profile. For details about how to configure an access profile, see **3.6.2 Configuring an Access Profile**.

When configuring NAC, pay attention to the following points:

- Layer 2 physical interfaces, Layer 3 physical interfaces, routed main interfaces, VLANIF interfaces, WAN-side interfaces, port groups, and VAP profiles support NAC. The support for authentication types on different interfaces is as follows:
  - Layer 2 physical interfaces: 802.1X authentication, MAC address authentication, and Layer 2 Portal authentication

    NOTE

    The Layer 2 physical interfaces of AR100&AR120&AR150&AR160&AR200 do not support Layer 2 Portal authentication, and support only 802.1X authentication in multicast mode.
  - Layer 3 physical interfaces and routed main interface: Layer 3 Portal authentication

    NOTE

    In wireless scenarios, it does not support Layer 3 Portal authentication.

 Copyright © Huawei Technologies Co., Ltd. 

  - VLANIF interfaces: Layer 2 Portal authentication, MAC address-prioritized Portal authentication in Fat AP Wi-Fi scenarios, and Layer 3 Portal authentication.
  - WAN-side interfaces: Layer 3 Portal authentication
- Physical interfaces do not support multi-mode authentication modes containing Portal authentication.
- For the access of wireless users through APs, ensure that the APs can be authenticated (for example, adding the APs to static users) when NAC authentication is deployed for users. Otherwise, the wireless users cannot be authenticated.
- NAC authentication cannot be enabled both on a Layer 2 Ethernet interface and the VLANIF interface mapping the VLAN of the Ethernet interface. Otherwise, the users have no network access rights after connecting to the network. In addition, NAC authentication cannot be enabled both on VAP profiles and VLANIF interfaces in wireless scenarios.
- After enabling NAC on an interface, you cannot run the following commands on the interface. Similarly, after running the following commands on an interface, you cannot enable NAC on the interface.

| Command | Function |
| --- | --- |
| **mac-limit** | Sets the maximum number of MAC addresses that can be learned by an interface. |
| **mac-address learning disable** | Disables MAC address learning on an interface. |
| **port-security enable** | Enables port security. |

## Prerequisites

An authentication profile has been configured. For details about how to configure an authentication profile, see **3.6.3 Configuring an Authentication Profile**.

## Procedure

- Enable NAC on an interface.
  a. Run **system-view**
     The system view is displayed.
  b. Run **interface** *interface-type interface-number*
     The interface view is displayed.
  c. Run **authentication-profile** *authentication-profile-name*
     The authentication profile is applied to the interface.
     By default, no authentication profile is applied to an interface.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

In wireless access scenario, pay attention to the following points:

- When an authentication profile is bound to a portal access profile, the authentication profile can be applied to VLANIF interface or WLAN-BSS interface (FAT-AP mode).
- When both MAC and portal access profiles are bound to an authentication profile and MAC address-prioritized Portal authentication is enabled, the authentication profile can only be applied to VLANIF interfaces.

- Enable NAC in a VAP profile.
  a. Run **system-view**

     The system view is displayed.
  b. Run **wlan**

     The WLAN view is displayed.
  c. Run **wlan ac**

     The WLAN view is displayed.
  d. Run **vap-profile name** *profile-name*

     The VAP profile view is displayed.
  e. Run **authentication-profile** *authentication-profile-name*

     The authentication profile is applied to the VAP profile.

     By default, no authentication profile is applied to a VAP profile.

**----End**

## Verifying the Configuration

Run the **display authentication interface** *interface-type interface-number* command to view the configuration of the NAC authentication mode on an interface.

# 3.6.5 (Optional) Configuring NAC Extended Functions

## 3.6.5.1 Configuring Extended Functions Related to 802.1X Authentication

### 3.6.5.1.1 Configuring the Interval for Sending 802.1X Authentication Requests

## Context

The device starts the **tx-period** timer (specifying the interval for sending 802.1X authentication requests) in either of the following situations:

- When a client initiates authentication, the device sends a unicast Request/Identity packet to the client and starts the **tx-period** timer. If the client does not respond within the period set by the timer, the device retransmits the authentication request.
- To authenticate the 802.1X clients that cannot initiate authentication, the device periodically sends multicast Request/Identity packets through the

 Copyright © Huawei Technologies Co., Ltd. 

802.1X-enabled interface to the clients at the interval set by the **tx-period** timer.

If a request packet has been sent for the maximum number of times (configured using the **dot1x retry** *max-retry-value* command) and no response is received from the client, the device stops sending the request packet.

Generally, if the client fails to be authenticated, the device starts a backup mechanism (Portal authentication or granting specified access permission), so that the client can continue to access the network. If MAC address bypass authentication is disabled, the value of the timeout timer for EAP-Request/Identity packets is calculated as follows:

Timer value = (*max-retry-value* + 1) x *tx-period-value*

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **dot1x timer tx-period** *tx-period-value*

The interval for sending 802.1X authentication requests is configured.

By default, the device sends 802.1X authentication requests at an interval of 30 seconds.

**----End**

### 3.6.5.1.2 Configuring 802.1X-based Fast Deployment

## Context

On an 802.1X network, the administrator has a large amount of workload in downloading and upgrading 802.1X client software for each client. The authentication-free network access and URL redirection functions can be configured to implement fast deployment of 802.1X clients.

Before an 802.1X authentication is successful, the client is allowed to access authentication-free resources. After URL redirection is configured and the server providing URL redirection belongs to the authentication-free resources, the device changes the URL address entered by a user to the specified URL (for example, the URL address of the 802.1X client download page). Therefore, the 802.1X client can be quickly configured.

## Prerequisite

The server providing the URL redirection service has been configured as authentication-free resource by using the **3.6.3.4 (Optional) Configuring Authentication Event Authorization Information** or **3.6.3.5.1 (Optional) Configuring Authorization Information for Authentication-free Users**.

## Procedure

**Step 1** Run **system-view**

 Copyright © Huawei Technologies Co., Ltd. 

The system view is displayed.

**Step 2** Run **dot1x url** *url-string*

The URL redirection for 802.1X authentication is configured.

By default, URL redirection for 802.1X authentication is not configured.

**----End**

## 3.6.5.2 Configuring Extended Functions Related to Portal Authentication

### 3.6.5.2.1 Configuring CNA Bypass for iOS Terminals

## Context

The iOS operating system provides the Captive Network Assistant (CNA) function. With the CNA function, the iOS terminals (including iPhone, iPad, and iMAC) automatically detects wireless network connectivity after associating with a wireless network. If the network connection cannot be set up, the iOS terminals ask users to enter user names and passwords. If users do not enter the user names and passwords, the iOS terminals automatically disconnect from the wireless network.

However, Portal authentication allows users to access certain resources before authentication is successful. If the iOS terminals are disconnected, users cannot access the specified resources. The CNA bypass function addresses this problem. If the users do not enter user names and passwords immediately, the CNA bypass function keeps the iOS terminals online before the Portal authentication is successful. Therefore, the iOS users are allowed to access authentication-free resources.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **portal captive-bypass enable**

The CNA bypass function is enabled for iOS terminals.

By default, the CNA bypass function is disabled for iOS terminals.

**----End**

### 3.6.5.2.2 Configuring the CNA Adaptive Function for iOS Terminals

## Context

Since WLANs are widely provided, users have a demand for quick and convenient authentication by using applications on mobile terminals, without entering user names and passwords. In such authentication mode, mobile terminals need to automatically display the application-based Portal authentication page and the applications need to communicate with the background server. Therefore, the mobile terminals must be connected to the WLANs during authentication.

 Copyright © Huawei Technologies Co., Ltd. 

iOS terminals such as iPhones, iPads, and iMac computers provide the Captive Network Assistant (CNA) function. This function automatically detects the network connection status after iOS terminals connect to WLANs. If the network is disconnected, the iOS terminals display a page prompting users to enter user names and passwords. If users do not enter the user names and passwords, the iOS terminals automatically disconnect from the WLANs. As a result, users cannot use applications on iOS terminals for authentication.

To solve the problem, enable the CNA adaptive function so that iOS terminals are redirected to the application-based Portal authentication page when they connect to WLANs. Users can click the link on the page to start specified applications to perform Portal authentication. If users do not start applications to perform authentication, they can still access authentication-free resources on the WLANs.

NOTE

Authentication-free resources accessed by users cannot contain the URL captive.apple.com; otherwise, terminals cannot automatically display the Portal authentication page.

If the Portal authentication page is of the HTTPS type, terminals can automatically display the Portal authentication page only when an HTTPS URL is used and the domain name certificate is valid.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **portal captive-adaptive enable**

The CNA adaptive function is enabled for iOS terminals.

By default, the CNA adaptive function is disabled for iOS terminals.

If you run both the **portal captive-adaptive enable** and **portal captive-bypass enable** commands, the command executed later takes effect.

**----End**

### 3.6.5.2.3 Configuring the Maximum Number of Portal Authentication Users Allowed on the Device

## Context

You can perform the following configurations to restrict the maximum number of Portal authentication users allowed on the device.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **portal max-user** *user-number*

The maximum number of Portal authentication users allowed on the device is configured.

 Copyright © Huawei Technologies Co., Ltd. 

By default, the maximum number of Portal authentication users allowed on the device is not restricted within the device's capacity.

**Step 3** (Optional) Run **portal user-alarm percentage** *percent-lower-value percent-upper-value*

The alarm thresholds for the Portal authentication user count percentage are configured.

By default, the lower alarm threshold for the Portal authentication user count percentage is 50, and the upper alarm threshold for the Portal authentication user count percentage is 100.

When the percentage of online Portal authentication users against the maximum number of users allowed on the device exceeds the upper alarm threshold, the device generates an alarm. When the percentage reaches or falls below the lower alarm threshold, the device clears the alarm.

**----End**

### 3.6.5.2.4 (Optional) Forcing Portal Authentication Users Offline When a 3G/LTE Link Is Disconnected

## Context

When the router functioning as a mobile Internet gateway is deployed on a bus or metro, only the users who pass Portal authentication can connect to the vehicle-mounted Wi-Fi network and access external networks using the 3G/LTE interface. After the 3G/LTE link is disconnected, the users are not disconnected in real time while they cannot access any web page immediately. This had a negative effect on user experience.

After you configure Portal authentication users to be forcibly disconnected on a 3G/LTE interface, the device forces the Portal authentication users offline when the 3G/LTE link is disconnected. The disconnected users can still access internal network resources of the router, which improves user experience.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface cellular** *interface-number*

The cellular interface view is displayed.

**Step 3** Run **cut web-authentication-user** [ **domain** *domain-name* | **ssid** *ssid* ]

The device is configured to force Portal authentication users offline when the 3G/LTE link is disconnected.

By default, the Portal authentication users are still online when the 3G/LTE link is disconnected.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

### 3.6.5.3 Configuring the Quiet Function

## Context

If a user frequently fails NAC authentication within a short period, system performance will be affected, and brute force attacks on the user name and password may occur.

After the quiet function is enabled, if the number of times that a user fails to be authenticated within 60s exceeds the upper limit, the device discards the user's authentication request packets for a period to avoid frequent authentication failures.

NOTE

When the number of quiet entries reaches the maximum number, the device does not allow new users who are not in the quiet table to access the network.

## Procedure

- Configure the quiet function for 802.1X authentication users.
  a. Run **system-view**
     The system view is displayed.
  b. Run **dot1x quiet-period**
     The quiet function is enabled for 802.1X authentication users.
     By default, the quiet function is enabled for 802.1X authentication users.
  c. (Optional) Run **dot1x quiet-times** *fail-times*
     The maximum number of authentication failures within 60 seconds before the device quiets an 802.1X authentication user is configured.
     By default, the maximum number of authentication failures is 10.
  d. (Optional) Run **dot1x timer quiet-period** *quiet-period-value*
     The quiet period is configured for 802.1X authentication users who fail to be authenticated.
     By default, the quiet period is 60 seconds for 802.1X authentication users who fail to be authenticated.
- Configure the quiet function for MAC address authentication users.

  NOTE

  The quiet function for MAC address authentication users takes effect only after the device is disabled from assigning network access rights to users in each phase before authentication succeeds using the **undo authentication event action authorize** command. In multi-mode authentication of MAC address authentication users, the quiet function for MAC address authentication users does not take effect.

  a. Run **system-view**
     The system view is displayed.
  b. (Optional) Run **mac-authen quiet-times** *fail-times*
     The maximum number of authentication failures within 60 seconds before the device quiets a MAC address authentication user is configured.
     By default, the maximum number of authentication failures is 10.

 Copyright © Huawei Technologies Co., Ltd. 

c. Run **mac-authen timer quiet-period** *quiet-period-value*

The quiet period is configured for MAC address authentication users who fail to be authenticated.

By default, the quiet period is 60 seconds for MAC address authentication users who fail to be authenticated. If the value of *quiet-period-value* is 0, the quiet function is disabled for MAC address authentication users.

- Configure the quiet function for Portal authentication users.
  a. Run **system-view**

  The system view is displayed.

  b. Run **portal quiet-period**

  The quiet function is enabled.

  By default, the quiet function is enabled for Portal authentication users.

  c. (Optional) Run **portal quiet-times** *fail-times*

  The maximum number of authentication failures within 60 seconds before the device quiets a Portal authentication user is configured.

  By default, the maximum number of authentication failures is 10.

  d. (Optional) Run **portal timer quiet-period** *quiet-period-value*

  The quiet period is configured for Portal authentication users who fail to be authenticated.

  By default, the quiet period is 60 seconds for Portal authentication users who fail to be authenticated.

**----End**

### 3.6.5.4 Configuring the Web Push Function

## Context

After a user is successfully authenticated, the device forcibly redirect the user to a web page when receiving the HTTP or HTTPS packet from the user who accesses web pages for the first time. In addition to pushing advertisement pages, the device can obtain user terminal information through the HTTP or HTTPS packets sent by the users, and apply the information to other services. There are two ways to push web pages:

1. URL: pushes the URL corresponding to the web page.
2. URL template: pushes the URL template. A URL template must be created. The URL template contains the URL of the pushed web page and URL parameters.

If an application program that actively sends HTTP or HTTPS packets is installed on the user terminal, the terminal has sent the HTTP or HTTPS packet before the user accesses a web page. Therefore, the user is unaware of the web page push process.

For HTTP and HTTPS packets, the forcible push function takes effect only when a redirection ACL is used. If the user table always contains redirection ACLs, a web page is forcibly pushed when HTTPS packets from users match redirection ACL rules. Usually, you can configure the RADIUS server to authorize the Huawei

 Copyright © Huawei Technologies Co., Ltd. 

extended RADIUS attribute **HW-Redirect-ACL** to users for redirection ACL implementation.

NOTE

Built-in Portal authentication does not support the web page push function.

When an AR router is connected to Fit APs, the user group priority configuration does not take effect for users who go online from the Fit APs.

## Procedure

- URL mode
  a. Run **system-view**
     The system view is displayed.
  b. Run **aaa**
     The AAA view is displayed.
  c. Run **domain** *domain-name*
     An AAA domain is created and the AAA domain view is displayed.
     The device has two default domains: **default** and **default_admin**. Common access users use the **default** domain and the administrator uses the **default_admin** domain.
  d. Run **force-push url** *url-address*
     The URL push function is enabled.
     By default, the URL push function is disabled.
- URL template mode
  a. Create and configure a URL template.
     i. Run **system-view**
        The system view is displayed.
     ii. Run **url-template name** *template-name*
        A URL template is created and the URL template view is displayed.
        By default, no URL template is created on the device.
     iii. Run **url** [ **push-only** ] *url-string* [ **ssid** *ssid* ]
        A pushed URL is configured.
        By default, no pushed URL is configured.
        The SSID that users associate with must be the same as that configured on the device; otherwise, the device cannot push URLs to users.
     iv. Run **url-parameter** { **ac-ip** *ac-ip-value* | **ac-mac** *ac-mac-value* | **ap-ip** *ap-ip-value* | **ap-mac** *ap-mac-value* | **redirect-url** *redirect-url-value* | **ssid** *ssid-value* | **sysname** *sysname-value* | **user-ipaddress** *user-ipaddress-value* | **user-mac** *user-mac-value* | **user-vlan** *user-vlan-value* | **esn** *esn-value* } *
        Parameters carried in the URL are configured.
        By default, a URL does not carry parameters.
     v. Run **url-parameter mac-address format delimiter** *delimiter* { **normal** | **compact** }

 Copyright © Huawei Technologies Co., Ltd. 

The MAC address format in the URL is configured.

By default, the MAC address format in a URL is XXXXXXXXXXXX.

vi. Run **parameter** { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } *

Characters in the URL are configured.

By default, the start character in a URL is a question mark (?), the assignment character is an equal sign (=), and the delimiter between parameters is an ampersand (&).

vii. Run **quit**

Return to the system view.

b. Run **aaa**

The AAA view is displayed.

c. Run **domain** *domain-name*

An AAA domain is created and the AAA domain view is displayed.

The device has two default domains: **default** and **default_admin**. Common access users use the **default** domain and the administrator uses the **default_admin** domain.

d. Run **force-push url-template** *template-name*

The URL template push function is enabled.

By default, the URL template push function is disabled.

**----End**

## 3.6.5.5 (Optional) Configuring HTTP-based Authentication and Accounting Functions

## Context

In traditional NAC scenarios, Portal and RADIUS authentication modes are often used for carriers and enterprises that require a complete authentication solution. In Internet access scenarios, access control devices need to connect to Internet or cloud servers. Therefore, they need to provide HTTP-based authentication and obtain user authorization information, including online duration, traffic usage, and bandwidth. After users access the Internet, the access control device periodically sends accounting packets to the authentication and accounting server. The server performs accounting for the users based on user traffic statistics. When the online duration or traffic usage exceeds authorization, the device forcibly disconnects the user and sends the disconnection message of the user to the authentication and accounting server.

NOTE

Only the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW that can work as a WLAN Fat AP support this configuration.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface wlan-bss** *wlan-bss-number*

A WLAN-BSS interface is created and the WLAN-BSS interface view is displayed.

**Step 3** Run **web-service access enable**

Authentication and accounting functions are enabled on the WLAN-BSS interface.

By default, authentication and accounting functions are disabled on a WLAN-BSS interface.

**Step 4** Run **quit**

Return to the system view.

**Step 5** Run **web-service aaa server** *url* **authorize-enable**

A URL is configured for the authentication and accounting server

By default, no URL is configured for the authentication and accounting server.

**Step 6** (Optional) Run **web-service accounting enable**

The device is enabled to send accounting packets to the authentication and accounting server.

By default, the device does not send accounting packets to the authentication and accounting server.

To perform accounting for users based on the volume of traffic destined for the Internet, use this command.

**Step 7** (Optional) Run **web-service accounting interval** *interval*

The interval at which the device sends accounting packets to the authentication and accounting server is configured.

By default, the device sends accounting packets to the authentication and accounting server at an interval of 30 seconds.

To enable the device to periodically send accounting packets to the authentication and accounting server, use this command.

NOTE

Before running the preceding command, run the **web-service accounting enable** command to enable the device to send accounting packets to the authentication and accounting server.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

### 3.6.5.6 Configuring the Maximum Number of Consecutive Authentication Failures

#### Context

You can perform the following operations to configure the maximum number of consecutive authentication failures allowed on the device.

#### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **authentication authen-fail fail-times** *fail-times*

The maximum number of consecutive authentication failures is configured.

By default, the maximum number of consecutive authentication failures is 1.

**----End**

### 3.6.5.7 Adjusting the Matching Order of ACL Rules

#### Context

By default, for NAC users, packets are matched with ACL rules in descending order by rule ID. That is, a larger rule ID indicates a higher priority of an ACL rule. You can adjust the matching order of ACL rules so that an ACL rule with a smaller rule ID has a higher priority.

#### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **access-user acl-priviledge-revert**

The device is configured to match packets with ACL rules in ascending order by rule ID. That is, a smaller rule ID indicates a higher priority of an ACL rule.

By default, the device matches packets with ACL rules in descending order by rule ID. That is, a larger rule ID indicates a higher priority of a rule.

The configuration takes effect only after the device is restarted.

**----End**

### 3.6.5.8 Configuring User Isolation

#### Context

To block mutual access between users of a group or between users of two groups, configure user isolation.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **user-group** *group-name* command to create a user group and enter the user group view.

**Step 3** Run the **user-isolated** { **inter-group** | **inner-group** } * command to configure intra-group and inter-group isolation.

By default, inter-group or intra-group isolation is not configured in a user group.

After users are authenticated and go online, the RADIUS server dynamically delivers user group information. In this situation, the inter-group or intra-group isolation configuration cannot be modified or deleted.

**----End**

## 3.6.5.9 Setting the Source Address of Offline Detection Packets

## Context

The device sends an ARP probe packet to check the user online status. If the user does not respond within a detection period, the device considers that the user is offline.

NOTE

- This function does not take effect for users who use Layer 3 Portal authentication.
- In normal situations, after a device sends an ARP probe packet with a default source IP address, online clients will immediately respond with ARP reply packets. If online clients do not respond with ARP reply packets, the device logs them out unexpectedly. To resolve this problem, use either of the following methods:
  - Run the **access-user arp-detect vlan** *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address* command to specify a VLAN ID, source IP address, and source MAC address for ARP probe packets.
  - Run the **authentication timer handshake-period** *handshake-period* command to increase the handshake period so that the device can detect gratuitous ARP packets that these clients send at an irregular period. Once the device detects such packets, it does not log them out.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Set the source address of offline detection packets.

- Run **access-user arp-detect default ip-address** *ip-address*

  The default source IP address of offline detection packets is set.

  By default, the default source IP address of offline detection packets is 0.0.0.0.
- Run **access-user arp-detect vlan** *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*

  The source IP address and source MAC address are specified for offline detection packets in a VLAN.

 Copyright © Huawei Technologies Co., Ltd. 

By default, the source IP address and source MAC address are not specified for offline detection packets in a VLAN.

You are advised to set the user gateway IP address and its corresponding MAC address as the source IP address and source MAC address of offline detection packets.

NOTE

The following source IP addresses used in offline detection packets are listed in descending order of priority:

1. IP address and MAC address of the VLANIF interface corresponding to the VLAN that users belong to and on the same network segment as users
2. Source IP address specified using the **access-user arp-detect vlan** *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address* command for offline detection packets in a specified VLAN
3. Default source IP address specified using the **access-user arp-detect default ip-address** *ip-address* command for offline detection packets

**----End**

## 3.6.5.10 Enabling the Device to Dynamically Adjust the Rate at Which It Processes Packets from NAC Users

### Context

When a lot of NAC users send authentication or log off requests to the device, the CPU usage may be overloaded especially when the CPU or memory usage is already high (for example, above 80%). After the device is enabled to dynamically adjust the rate of packets from NAC users, the device limits the number of NAC packets received per second if the CPU or memory usage is high. This function reduces loads on the device CPU.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **authentication speed-limit auto**

The device is enabled to dynamically adjust the rate at which it processes packets from NAC users.

**----End**

## 3.6.5.11 Enabling URL Encoding and Decoding

### Context

To improve web application security, data from untrustworthy sources must be encoded before being sent to clients. URL encoding is most commonly used in web applications. After URL encoding and decoding are enabled, some special characters in redirected URLs are converted to secure formats, preventing clients from mistaking them for syntax signs or instructions and unexpectedly modifying

 Copyright © Huawei Technologies Co., Ltd. 

the original syntax. In this way, cross-site scripting attacks and injection attacks are prevented.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **portal url-encode enable**

URL encoding and decoding are enabled.

By default, URL encoding and decoding are enabled.

**----End**

### Check the Configuration

Run the **display portal url-encode configuration** command to check the configuration of URL encoding and decoding.

## 3.6.5.12 Verifying the NAC Extended Functions Configuration

### Context

After configuring extended functions, run the following commands to check the configuration.

### Procedure

- Run the **display portal quiet-user** { **all** | **user-ip** *ip-address* | **server-ip** *ip-address* } command to check information about Portal authentication users who are quieted.
- Run the **display mac-authen quiet-user** { **all** | **mac-address** *mac-address* } command to check information about MAC address authentication users who are quieted.
- Run the **display dot1x quiet-user** { **all** | **mac-address** *mac-address* } command to check information about 802.1X authentication users who are quieted.

**----End**

# 3.7 Maintaining NAC

## 3.7.1 Configuring the NAC Alarm Report Function

### Context

You can configure the NAC alarm report function, which helps you obtain real-time running status of the NAC network and facilitates operation and maintenance.

 Copyright © Huawei Technologies Co., Ltd. 

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **snmp-agent trap enable feature-name mid_eapol** [ **trap-name** { **hwmacauthenmaxuseralarm** | **hwsrvcfgeapmaxuseralarm** } ]

The trap function is enabled for the DOT1X module.

By default, the trap function is enabled for the DOT1X module.

**Step 3** Run **snmp-agent trap enable feature-name mid_web** [ **trap-name** { **hwportalmaxuseralarm** | **hwportaluserclearalarm** | **hwportalserverdown** | **hwportalserverup** } ]

The trap function is enabled for the web authentication module.

By default, the trap function is enabled for the web authentication module.

**----End**

### Verifying the Configuration

- Run the **display snmp-agent trap feature-name mid_eapol all** command to check information about all traps on the DOT1X module.
- Run the **display snmp-agent trap feature-name mid_web all** command to check information about all traps on the web authentication module.

## 3.7.2 Clearing NAC Statistics

### Context

NOTICE

Cleared statistics cannot be restored. Exercise caution when you run the following commands.

### Procedure

- Run the **reset dot1x statistics** command in the user view to clear statistics about 802.1X authentication.
- Run the **reset mac-authen statistics** command in the user view to clear statistics about MAC address authentication.

**----End**

## 3.7.3 Monitoring NAC Operation

### Context

In routine maintenance, you can run the following commands in any view to check whether NAC is functioning properly.

 Copyright © Huawei Technologies Co., Ltd. 

### Procedure

- Run the **display access-user** command to view information about NAC access users.
- Run the **display dot1x** command to view information about 802.1X authentication.
- Run the **display mac-authen** command to view information about MAC address authentication.
- Run the **display portal** command to view information about Portal authentication.
- Run the **display portal local-server connect** command to view the connection status of users to be authenticated on a built-in Portal server.
- Run the **display server-detect state** command to view the status of a Portal server.
- Run the **display mac-address authen** command to view MAC address entries of the **authen** type in the system.
- Run the **display mac-address pre-authen** command to view MAC address entries of the **Pre-authen** type in the system.
- Run the **display user-group** [ *group-name* ] command to view the configuration of a user group.

**----End**

# 3.8 Configuration Examples for NAC

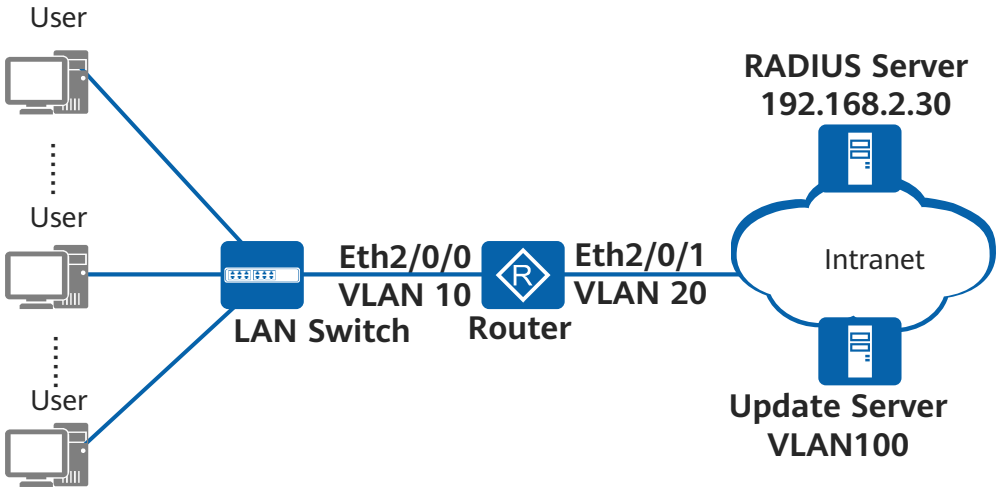
## 3.8.1 Example for Configuring 802.1X Authentication

### Networking Requirements

As shown in **Figure 3-12**, many users on a company access network through Eth2/0/0 of the Router (used as an access device). After the network operates for a period of time, attacks are detected. The administrator must control network access rights of user terminals to ensure network security. The Router allows user terminals to access Internet resources only after they are authenticated.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 3-12** Networking diagram for configuring 802.1X authentication




## Configuration Roadmap

To control the network access permission of users, the administrator can configure 802.1X authentication on the Router after the server with the IP address 192.168.2.30 is used as the RADIUS server.

The configuration roadmap is as follows (configured on the Router):

1. Create and configure a RADIUS server template, an AAA scheme, and an ISP domain. Bind the RADIUS server template and the AAA scheme to the ISP domain. The Router can then exchange information with the RADIUS server.
2. Configure 802.1X authentication to control network access rights of the employees in offices. The configuration includes:
   a. Configure an 802.1X access profile.
   b. Configure an authentication profile.
   c. Enable 802.1X authentication on an interface.

NOTE

Before performing operations in this example, ensure that user access terminals and the server can communicate.

This example only provides the configurations on the Router. The configurations on the LAN switch and RADIUS server are not provided here.

## Procedure

**Step 1** Create VLANs and configure the VLAN allowed by the interface to ensure network communication.

# Create VLAN 10 and VLAN 20.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10 20
```

# On the Router, set Eth2/0/0 connecting to users as an access interface, and add Eth2/0/0 to VLAN 10.

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type access
[Router-Ethernet2/0/0] port default vlan 10
[Router-Ethernet2/0/0] quit
```

NOTE

Configure the interface type and VLANs according to the actual situation. In this example, users are added to VLAN 10.

# On the Router, set Eth2/0/1 connecting to the RADIUS server as an access interface, and add Eth2/0/1 to VLAN 20.

```
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type access
[Router-Ethernet2/0/1] port default vlan 20
[Router-Ethernet2/0/1] quit
```

**Step 2** Create and configure a RADIUS server template, an AAA scheme, and an authentication domain.

# Create and configure RADIUS server template **rd1**.

```
[Router] radius-server template rd1
[Router-radius-rd1] radius-server authentication 192.168.2.30 1812
[Router-radius-rd1] radius-server shared-key cipher Huawei@2012
[Router-radius-rd1] quit
```

# Create AAA scheme **abc** and set the authentication mode to RADIUS.

```
[Router] aaa
[Router-aaa] authentication-scheme abc
[Router-aaa-authen-abc] authentication-mode radius
[Router-aaa-authen-abc] quit
```

# Create authentication domain **isp1**, and bind AAA scheme **abc** and RADIUS server template **rd1** to authentication domain **isp1**.

```
[Router-aaa] domain isp1
[Router-aaa-domain-isp1] authentication-scheme abc
[Router-aaa-domain-isp1] radius-server rd1
[Router-aaa-domain-isp1] quit
[Router-aaa] quit
```

# Test whether a user can be authenticated using RADIUS authentication. A user name **test@huawei.com** and password **Huawei2012** have been configured on the RADIUS server.

```
[Router] test-aaa test@huawei.com Huawei2012 radius-template rd1
Info: Account test succeed.
```

**Step 3** Configure 802.1X authentication.

# Configure the 802.1X access profile **d1**.

NOTE

By default, an 802.1X access profile uses the EAP authentication mode. Ensure that the RADIUS server supports EAP; otherwise, the server cannot process 802.1X authentication request packets.

```
[Router] dot1x-access-profile name d1
[Router-dot1x-access-profile-d1] quit
```

# Configure the authentication profile **p1**, bind the 802.1X access profile **d1** to the authentication profile, and specify the domain **isp1** as the forcible authentication domain in the authentication profile.

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router] authentication-profile name p1
[Router-authen-profile-p1] dot1x-access-profile d1
[Router-authen-profile-p1] access-domain isp1 force
[Router-authen-profile-p1] quit
```

# Bind the authentication profile **p1** to Eth2/0/0 and enable 802.1X authentication on the interface.

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] authentication-profile p1
[Router-Ethernet2/0/0] quit
```

**Step 4** Verify the configuration.

1. Run the **display dot1x** command to check the 802.1X authentication configuration. The command output (**802.1X protocol is Enabled**) shows that the 802.1X authentication has been enabled on the interface Eth2/0/0.
2. The user starts the 802.1X client on the terminal, and enters the user name and password for authentication.
3. If the user name and password are correct, an authentication success message is displayed on the client page. The user can access the network.
4. After the user goes online, you can run the **display access-user** command on the device to check the online 802.1X user information.

**----End**

## Configuration Files

Router configuration file

```
#
sysname Router
#
vlan batch 10 20
#
authentication-profile name p1
 dot1x-access-profile d1
 access-domain isp1 force
#
radius-server template rd1
 radius-server shared-key cipher %^%#5Cz2!R*M%NaEr^6.].')L/$!!xTKZ<!!!!!!!!!!%^%#
 radius-server authentication 192.168.2.30 1812 weight 80
#
aaa
 authentication-scheme abc
  authentication-mode radius
 domain isp1
  authentication-scheme abc
  radius-server rd1
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 10
 authentication-profile p1
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 20
#
dot1x-access-profile name d1
#
return
```

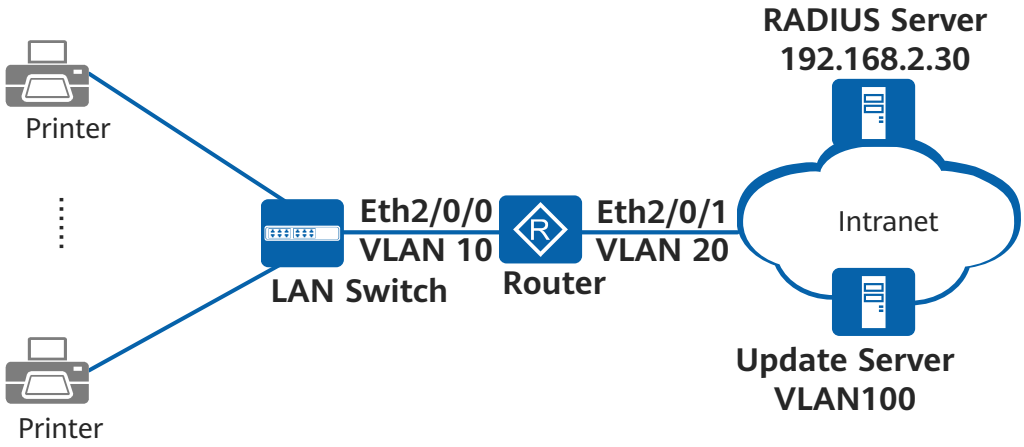
 Copyright © Huawei Technologies Co., Ltd. 

# 3.8.2 Example for Configuring MAC Address Authentication

## Networking Requirements

As shown in **Figure 3-13**, many printers on a company access network through Eth2/0/0 of the Router (used as an access device). After the network operates for a period of time, the administrator controls the network access rights of the printers to improve network security. The Router allows a printer to access Internet resources only after the printer is authenticated.

**Figure 3-13** Networking diagram for configuring MAC address authentication




## Configuration Roadmap

Printers cannot install and use the 802.1X client. The administrator can configure MAC address authentication on the Router to control the network access rights of the printers.

The configuration roadmap is as follows (configured on the Router):

1. Create and configure a RADIUS server template, an AAA scheme, and an ISP domain; bind the RADIUS server template and the AAA scheme to the ISP domain. The Router can then exchange information with the RADIUS server.
2. Configure MAC address authentication so that the Switch can control network access rights of the dumb terminals. The configuration includes:
   a. Configure a MAC access profile.
   b. Configure an authentication profile.
   c. Enable MAC address authentication on an interface.

NOTE

Before performing operations in this example, ensure that user access terminals and the server can communicate.

This example only provides the configurations on the Router. The configurations on the LAN switch and RADIUS server are not provided here.


Copyright © Huawei Technologies Co., Ltd.

## Procedure

**Step 1** Create VLANs and configure the VLAN allowed by the interface to ensure network communication.

# Create VLAN 10 and VLAN 20.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10 20
```

# On the Router, set Eth2/0/0 connecting to users as an access interface, and add Eth2/0/0 to VLAN 10.

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type access
[Router-Ethernet2/0/0] port default vlan 10
[Router-Ethernet2/0/0] quit
```

NOTE

Configure the interface type and VLANs according to the actual situation. In this example, users are added to VLAN 10.

# On the Router, set Eth2/0/1 connecting to the RADIUS server as an access interface, and add Eth2/0/1 to VLAN 20.

```
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type access
[Router-Ethernet2/0/1] port default vlan 20
[Router-Ethernet2/0/1] quit
```

**Step 2** Create and configure a RADIUS server template, an AAA scheme, and an authentication domain.

# Create and configure RADIUS server template **rd1**.

```
[Router] radius-server template rd1
[Router-radius-rd1] radius-server authentication 192.168.2.30 1812
[Router-radius-rd1] radius-server shared-key cipher Huawei@2012
[Router-radius-rd1] quit
```

# Create AAA scheme **abc** and set the authentication mode to RADIUS.

```
[Router] aaa
[Router-aaa] authentication-scheme abc
[Router-aaa-authen-abc] authentication-mode radius
[Router-aaa-authen-abc] quit
```

# Create authentication domain **isp1**, and bind AAA scheme **abc** and RADIUS server template **rd1** to authentication domain **isp1**.

```
[Router-aaa] domain isp1
[Router-aaa-domain-isp1] authentication-scheme abc
[Router-aaa-domain-isp1] radius-server rd1
[Router-aaa-domain-isp1] quit
[Router-aaa] quit
```

# Test whether a user can be authenticated using RADIUS authentication. A user name **test@huawei.com** and password **Huawei2012** have been configured on the RADIUS server.

```
[Router] test-aaa test@huawei.com Huawei2012 radius-template rd1
Info: Account test succeed.
```

**Step 3** Configure MAC address authentication.

 Copyright © Huawei Technologies Co., Ltd. 

# Configure the MAC access profile **m1**.

NOTE

In a MAC access profile, a MAC address without hyphens (-) is used as the user name and password for MAC address authentication. Ensure that the formats of the user name and password for MAC address authentication configured on the RADIUS server are the same as those configured on the access device.

```
[Router] mac-access-profile name m1
[Router-mac-access-profile-m1] quit
```

# Configure the authentication profile **p1**, bind the MAC access profile **m1** to the authentication profile, and specify the domain **isp1** as the forcible authentication domain in the authentication profile.

```
[Router] authentication-profile name p1
[Router-authen-profile-p1] mac-access-profile m1
[Router-authen-profile-p1] access-domain isp1 force
[Router-authen-profile-p1] quit
```

# Bind the authentication profile **p1** to Eth2/0/0 and enable MAC address authentication on the interface.

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] authentication-profile p1
[Router-Ethernet2/0/0] quit
```

**Step 4** Verify the configuration.

1. Run the **display mac-authen** command to check the MAC address authentication configuration. The command output (**MAC address authentication is enabled**) shows that MAC address authentication has been enabled on the interface Eth2/0/0.
2. After the user starts the terminal, the device automatically obtains the terminal MAC address and uses it as the user name and password for authentication.
3. The user can access the network after the authentication succeeds.
4. After the user goes online, you can run the **display access-user** command on the device to check the online MAC address authentication user information.

**----End**

## Configuration Files

Router configuration file

```
#
sysname Router
#
vlan batch 10 20
#
authentication-profile name p1
 mac-access-profile m1
 access-domain isp1 force
#
radius-server template rd1
 radius-server shared-key cipher %^%#5Cz2!R*M%NaEr^6.]')L/$!!xTKZ<!!!!!!!!!!%^%#
 radius-server authentication 192.168.2.30 1812 weight 80
#
aaa
 authentication-scheme abc
  authentication-mode radius
```

```
 domain isp1
  authentication-scheme abc
  radius-server rd1
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 10
 authentication-profile p1
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 20
#
mac-access-profile name m1
#
return
```

# 3.8.3 Example for Configuring Layer 2 External Portal Authentication

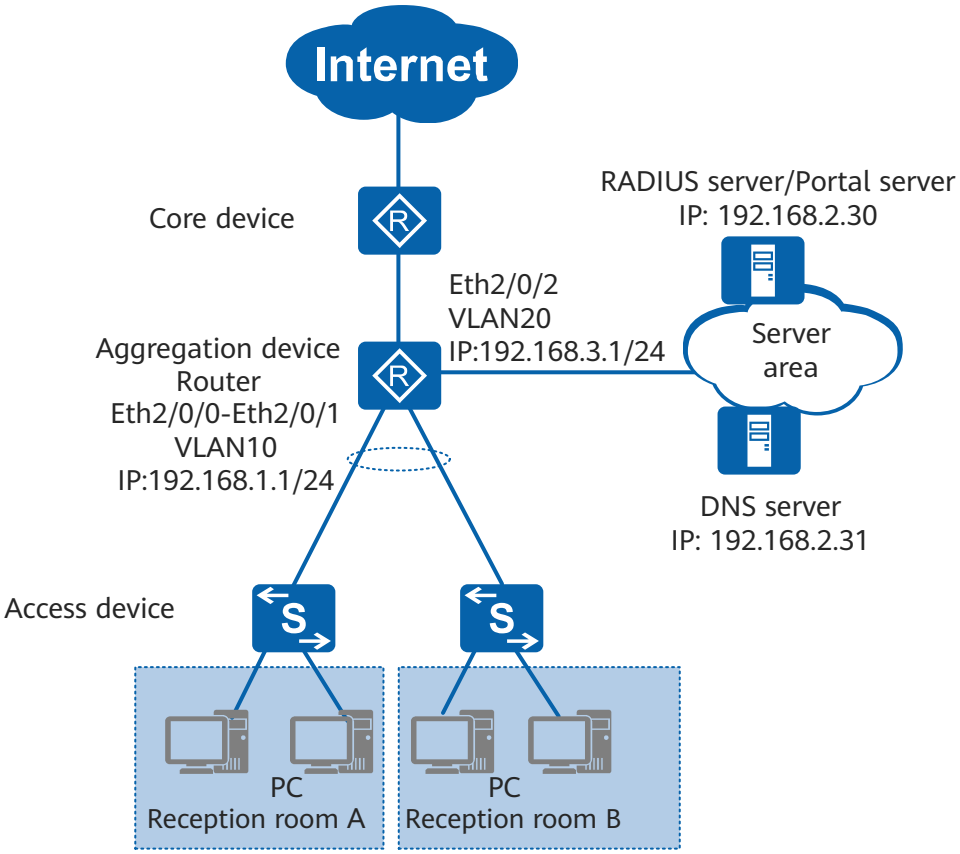
## Networking Requirements

As shown in **Figure 3-14**, an enterprise needs to deploy an identity authentication system in reception rooms to implement access control on visitors who attempt to connect to the enterprise network, ensuring that only authenticated users can access the network. Because the reception rooms have medium security requirements, you do not need to deploy too many authentication points. It is required that the authentication control point be deployed on the aggregation device to facilitate maintenance.

Portal authentication features flexible deployment and is applicable to moving users. The aggregation router and visitors' terminals communicate at Layer 2. Therefore, you can deploy Layer 2 Portal authentication on the aggregation router. The aggregation router works with the RADIUS server (integrated with the Portal server) to implement access control on visitors who attempt to connect to the enterprise network.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 3-14** Networking diagram for configuring Layer 2 external Portal authentication




## Configuration Roadmap

The following configurations are performed on the aggregation router. The configuration roadmap is as follows:

1. Configure network interconnections.
2. Configure AAA on the router to implement identity authentication on access users through the RADIUS server. The configuration includes configuring a RADIUS server template, an AAA scheme, and an authentication domain, and binding the RADIUS server template and AAA scheme to the authentication domain.
3. Configure Portal authentication to control network access rights of the visitors in the visitor area. The configuration includes:
   a. Configure a Portal server template.
   b. Configure a Portal access profile.
   c. Configure an authentication-free rule profile.
   d. Configure an authentication profile.
   e. Enable Portal authentication on an interface.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

Before performing operations in this example, ensure that user access terminals and the server can communicate.

This example only provides the configurations on the Router. The configurations on the LAN switch and RADIUS server are not provided here.

Parameters including the RADIUS authentication shared key, RADIUS accounting shared key, Portal shared key, accounting interval, and port number must be kept consistent on the router and server.

## Procedure

**Step 1** Create VLANs and configure the allowed VLANs on interfaces to ensure network connectivity.

# Create VLAN 10 and VLAN 20.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10 20
```

# On the router, configure Eth2/0/0 and Eth2/0/1 connecting to users as access interfaces, and add Eth2/0/0 and Eth2/0/1 to VLAN 10.

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type access
[Router-Ethernet2/0/0] port default vlan 10
[Router-Ethernet2/0/0] quit
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type access
[Router-Ethernet2/0/1] port default vlan 10
[Router-Ethernet2/0/1] quit
```

# On the router, configure Eth2/0/2 connecting to the RADIUS server as an access interface, and add Eth2/0/2 to VLAN 20.

```
[Router] interface ethernet 2/0/2
[Router-Ethernet2/0/2] port link-type access
[Router-Ethernet2/0/2] port default vlan 20
[Router-Ethernet2/0/2] quit
```

**Step 2** Configure IP addresses for VLANIF 10 and VLANIF 20.

```
[Router] interface vlanif 10
[Router-Vlanif10] ip address 192.168.1.1 24
[Router-Vlanif10] quit
```

```
[Router] interface vlanif 20
[Router-Vlanif20] ip address 192.168.3.1 24
[Router-Vlanif20] quit
```

**Step 3** Configure the DHCP server to assign IP addresses to terminals and notify the terminals of the DNS server address.

```
[Router] dhcp enable
[Router] interface vlanif 10
[Router-Vlanif10] dhcp select interface
[Router-Vlanif10] dhcp server dns-list 192.168.2.31
[Router-Vlanif10] quit
```

**Step 4** Configure a static route to the server area. In this example, the IP address for the server area to connect to the router is 192.168.2.1.

```
[Router] ip route-static 192.168.2.0 255.255.255.0 192.168.2.1
```

**Step 5** Create and configure a RADIUS server template, an AAA authentication scheme, and an authentication domain.

 Copyright © Huawei Technologies Co., Ltd. 

# Create and configure the RADIUS server template **rd1**.

```
[Router] radius-server template rd1
[Router-radius-rd1] radius-server authentication 192.168.2.30 1812
[Router-radius-rd1] radius-server shared-key cipher Huawei@2012
[Router-radius-rd1] quit
```

# Create the AAA authentication scheme **abc** and set the authentication mode to RADIUS.

```
[Router] aaa
[Router-aaa] authentication-scheme abc
[Router-aaa-authen-abc] authentication-mode radius
[Router-aaa-authen-abc] quit
```

# Create the authentication domain **isp1**, and bind the AAA authentication scheme **abc** and RADIUS server template **rd1** to the domain.

```
[Router-aaa] domain isp1
[Router-aaa-domain-isp1] authentication-scheme abc
[Router-aaa-domain-isp1] radius-server rd1
[Router-aaa-domain-isp1] quit
[Router-aaa] quit
```

# Check whether a user can pass RADIUS authentication. (The test user **test@huawei.com** and password **Huawei2012** have been configured on the RADIUS server.)

```
[Router] test-aaa test@huawei.com Huawei2012 radius-template rd1
Info: Account test succeed.
```

**Step 6** Configure Portal authentication.

# Configure the Portal server template **abc**.

```
[Router] web-auth-server abc
[Router-web-auth-server-abc] server-ip 192.168.2.30
[Router-web-auth-server-abc] port 50200
[Router-web-auth-server-abc] url http://192.168.2.30:8080/webagent
[Router-web-auth-server-abc] shared-key cipher Huawei@123
[Router-web-auth-server-abc] quit
```

# Configure the Portal access profile **web1**.

```
[Router] portal-access-profile name web1
[Router-portal-acces-profile-web1] web-auth-server abc direct
[Router-portal-acces-profile-web1] quit
```

# Configure the authentication-free rule profile **default_free_rule** to allow packets to the DNS server to pass through.

```
[Router] free-rule-template name default_free_rule
[Router-free-rule-default_free_rule] free-rule 1 destination ip 192.168.2.31 mask 32
[Router-free-rule-default_free_rule] quit
```

**NOTE**

Authentication-free rules can take effect immediately after being configured in an authentication-free profile. It is unnecessary to bind the authentication-free profile to an authentication profile.

# Configure the authentication profile **p1**, bind the Portal access profile **web1** and authentication-free rule profile **default_free_rule** to the authentication profile, and specify the domain **isp1** as the forcible authentication domain in the authentication profile.

```
[Router] authentication-profile name p1
[Router-authen-profile-p1] portal-access-profile web1
[Router-authen-profile-p1] access-domain isp1 force
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router-authen-profile-p1] free-rule-template default_free_rule
[Router-authen-profile-p1] quit
```

# Bind the authentication profile **p1** to VLANIF 10 and enable Portal authentication on the interface.

```
[Router] interface vlanif 10
[Router-Vlanif10] authentication-profile p1
[Router-Vlanif10] quit
```

**Step 7** Verify the configuration.

1. Run the **display portal** and **display web-auth-server configuration** commands to view the configuration of external Portal authentication. The **web-auth-server layer2(direct)** field in the command output shows that the Portal server template has been bound to VLANIF 10.
2. After a user opens the browser and enters any website address, the user will be redirected to the Portal authentication page. The user then can enter the user name and password for authentication.
3. If the user name and password are correct, an authentication success message is displayed on the Portal authentication page. The user can access the network.
4. After users go online, you can run the **display access-user** command on the device to view information about online Portal authentication users.

**----End**

## Configuration Files

Router configuration file

```
#
sysname Router
#
vlan batch 10 20
#
authentication-profile name p1
 portal-access-profile web1
 free-rule-template default_free_rule
 access-domain isp1 force
#
dhcp enable
#
radius-server template rd1
 radius-server shared-key cipher %^%#5Cz2!R*M%NaEr^6.]')L/$!!xTKZ<!!!!!!!!!!%^%#
 radius-server authentication 192.168.2.30 1812 weight 80
#
free-rule-template name default_free_rule
 free-rule 1 destination ip 192.168.2.31 mask 255.255.255.255
#
web-auth-server abc
 server-ip 192.168.2.30
 port 50200
 shared-key cipher %^%#'=oP;*.KKUSPqB7M5Cf2G)!!!t/&,$!!!!!!!!!!%^%#
 url http://192.168.2.30:8080/webagent
#
portal-access-profile name web1
 web-auth-server abc direct
#
aaa
 authentication-scheme abc
  authentication-mode radius
 domain isp1
  authentication-scheme abc
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 radius-server rd1
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
 authentication-profile p1
 dhcp select interface
 dhcp server dns-list 192.168.2.31
#
interface Vlanif20
 ip address 192.168.3.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 10
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 10
#
interface Ethernet2/0/2
 port link-type access
 port default vlan 20
#
ip route-static 192.168.2.0 255.255.255.0 192.168.2.1
#
return
```

# 3.8.4 Example for Configuring Layer 3 External Portal Authentication

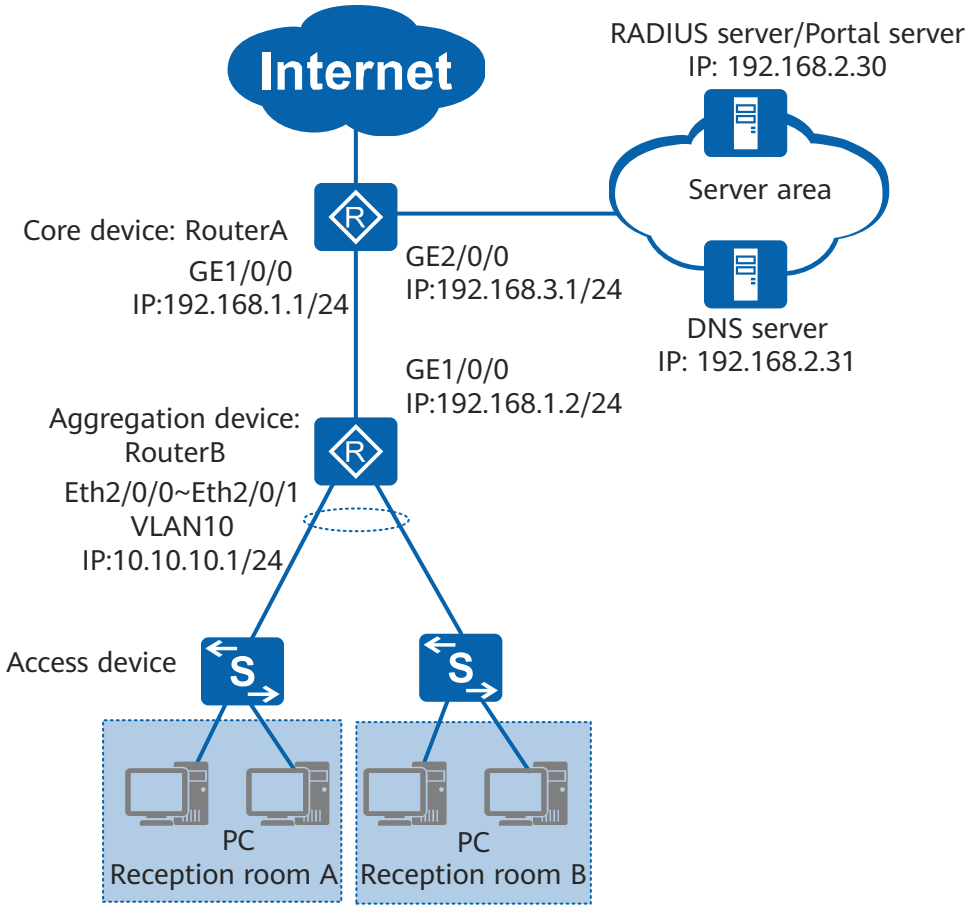
## Networking Requirements

As shown in **Figure 3-15**, an enterprise needs to deploy an identity authentication system in reception rooms to implement access control on visitors who attempt to connect to the enterprise network, ensuring that only authenticated users can access the network. To facilitate future network reconstruction and save investment, it is required that the authentication control point be deployed on the core device.

Portal authentication features flexible deployment and is applicable to moving users. The core device RouterA and visitors' terminals communicate at Layer 3. Therefore, you can deploy Layer 3 Portal authentication on the core device RouterA. RouterA works with the RADIUS server (integrated with the Portal server) to implement access control on visitors who attempt to connect to the enterprise network.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 3-15** Networking diagram for configuring Layer 3 external Portal authentication




## Configuration Roadmap

The following configurations are performed on RouterA. The configuration roadmap is as follows:

1. Configure network interconnections.
2. Configure AAA on RouterA to implement identity authentication on access users through the RADIUS server. The configuration includes configuring a RADIUS server template, an AAA scheme, and an authentication domain, and binding the RADIUS server template and AAA scheme to the authentication domain.
3. Configure Portal authentication to control network access rights of the visitors in the visitor area. The configuration includes:
   a. Configure a Portal server template.
   b. Configure a Portal access profile.
   c. Configure an authentication-free rule profile.
   d. Configure an authentication profile.

 Copyright © Huawei Technologies Co., Ltd. 

e. Enable Portal authentication on an interface.

**NOTE**

Before performing operations in this example, ensure that user access terminals and the server can communicate.

This example only provides the configurations on the Router. The configurations on the LAN switch and RADIUS server are not provided here.

Parameters including the RADIUS authentication shared key, RADIUS accounting shared key, Portal shared key, accounting interval, and port number must be kept consistent on the router and server.

## Procedure

**Step 1** Configure RouterB to ensure network connectivity.

# Create VLAN 10.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] vlan batch 10
```

# On RouterB, configure Eth2/0/0 and Eth2/0/1 connecting to users as access interfaces, and add Eth2/0/0 and Eth2/0/1 to VLAN 10.

```
[RouterB] interface ethernet 2/0/0
[RouterB-Ethernet2/0/0] port link-type access
[RouterB-Ethernet2/0/0] port default vlan 10
[RouterB-Ethernet2/0/0] quit
[RouterB] interface ethernet 2/0/1
[RouterB-Ethernet2/0/1] port link-type access
[RouterB-Ethernet2/0/1] port default vlan 10
[RouterB-Ethernet2/0/1] quit
```

# On RouterB, configure an IP address for GE1/0/0 connecting to RouterA.

```
[RouterB] interface gigabitEthernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 192.168.1.2 24
[RouterB-GigabitEthernet1/0/0] quit
```

# Configure an IP address for VLANIF 10 and configure VLANIF 10 as the DHCP relay agent.

```
[RouterB] dhcp enable
[RouterB] interface vlanif 10
[RouterB-Vlanif10] ip address 10.10.10.1 24
[RouterB-Vlanif10] dhcp select relay
[RouterB-Vlanif10] dhcp relay server-ip 192.168.1.1
[RouterB-Vlanif10] quit
```

# Configure the default route.

```
[RouterB] ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
```

**Step 2** Configure RouterA to ensure network connectivity.

# On RouterA, configure an IP address for GE1/0/0 connecting to RouterB.

```
[RouterA] interface gigabitEthernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
```

# On RouterA, configure an IP address for GE2/0/0 connecting to the server area.

 Copyright © Huawei Technologies Co., Ltd. 

```
[RouterA] interface gigabitEthernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 192.168.3.1 24
[RouterA-GigabitEthernet2/0/0] quit
```

# Enable the DHCP server function, and configure the DHCP server to assign IP addresses to terminals and notify the terminals of the DNS server address and gateway address.

```
[RouterA] dhcp enable
[RouterA] ip pool pool1
[RouterA-ip-pool-pool1] network 10.10.10.0 mask 24
[RouterA-ip-pool-pool1] gateway-list 10.10.10.1
[RouterA-ip-pool-pool1] dns-list 192.168.2.31
[RouterA-ip-pool-pool1] quit
[RouterA] interface gigabitEthernet 1/0/0
[RouterA-GigabitEthernet1/0/0] dhcp select global
[RouterA-GigabitEthernet1/0/0] quit
```

# Configure static routes from RouterA to user terminals and the server area, respectively. In this example, the IP address for the server area to connect to RouterA is 192.168.2.1.

```
[RouterA] ip route-static 10.10.10.0 255.255.255.0 192.168.1.2
[RouterA] ip route-static 192.168.2.0 255.255.255.0 192.168.2.1
```

**Step 3** Create and configure a RADIUS server template, an AAA authentication scheme, and an authentication domain.

# Create and configure the RADIUS server template **rd1**.

```
[RouterA] radius-server template rd1
[RouterA-radius-rd1] radius-server authentication 192.168.2.30 1812
[RouterA-radius-rd1] radius-server shared-key cipher Huawei@2012
[RouterA-radius-rd1] quit
```

# Create the AAA authentication scheme **abc** and set the authentication mode to RADIUS.

```
[RouterA] aaa
[RouterA-aaa] authentication-scheme abc
[RouterA-aaa-authen-abc] authentication-mode radius
[RouterA-aaa-authen-abc] quit
```

# Create the authentication domain **isp1**, and bind the AAA authentication scheme **abc** and RADIUS server template **rd1** to the domain.

```
[RouterA-aaa] domain isp1
[RouterA-aaa-domain-isp1] authentication-scheme abc
[RouterA-aaa-domain-isp1] radius-server rd1
[RouterA-aaa-domain-isp1] quit
[RouterA-aaa] quit
```

# Check whether a user can pass RADIUS authentication. (The test user **test@huawei.com** and password **Huawei2012** have been configured on the RADIUS server.)

```
[RouterA] test-aaa test@huawei.com Huawei2012 radius-template rd1
Info: Account test succeed.
```

**Step 4** Configure Portal authentication.

# Configure the Portal server template **abc**.

```
[RouterA] web-auth-server abc
[RouterA-web-auth-server-abc] server-ip 192.168.2.30
[RouterA-web-auth-server-abc] port 50200
[RouterA-web-auth-server-abc] url http://192.168.2.30:8080/webagent
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[RouterA-web-auth-server-abc] shared-key cipher Huawei@123
[RouterA-web-auth-server-abc] quit
```

# Configure the Portal access profile **web1**.

```
[RouterA] portal-access-profile name web1
[RouterA-portal-acces-profile-web1] web-auth-server abc layer3
[RouterA-portal-acces-profile-web1] quit
```

# Configure the authentication-free rule profile **default_free_rule** to allow packets to the DNS server and DHCP server to pass through.

```
[RouterA] free-rule-template name default_free_rule
[RouterA-free-rule-default_free_rule] free-rule 1 destination ip 192.168.2.31 mask 32
[RouterA-free-rule-default_free_rule] free-rule 2 destination ip 192.168.1.1 mask 32
[RouterA-free-rule-default_free_rule] quit
```

**NOTE**

Authentication-free rules can take effect immediately after being configured in an authentication-free profile. It is unnecessary to bind the authentication-free profile to an authentication profile.

# Configure the authentication profile **p1**, bind the Portal access profile **web1** and authentication-free rule profile **default_free_rule** to the authentication profile, and specify the domain **isp1** as the forcible authentication domain in the authentication profile.

```
[RouterA] authentication-profile name p1
[RouterA-authen-profile-p1] portal-access-profile web1
[RouterA-authen-profile-p1] access-domain isp1 force
[RouterA-authen-profile-p1] free-rule-template default_free_rule
[RouterA-authen-profile-p1] quit
```

# Bind the authentication profile **p1** to GE1/0/0 and enable Portal authentication on the interface.

```
[RouterA] interface gigabitEthernet 1/0/0
[RouterA-GigabitEthernet1/0/0] authentication-profile p1
[RouterA-GigabitEthernet1/0/0] quit
```

**Step 5** Verify the configuration.

1. Run the **display portal** and **display web-auth-server configuration** commands on RouterA to view the configuration of external Portal authentication. The **web-auth-server layer3** field in the command output shows that the Portal server template has been bound to GE1/0/0.
2. After a user opens the browser and enters any website address, the user will be redirected to the Portal authentication page. The user then can enter the user name and password for authentication.
3. If the user name and password are correct, an authentication success message is displayed on the Portal authentication page. The user can access the network.
4. After users go online, you can run the **display access-user** command on RouterA to view information about online Portal authentication users.

**----End**

## Configuration Files

- RouterA configuration file

```
#
sysname RouterA
```

 Copyright © Huawei Technologies Co., Ltd. 

```
#
authentication-profile name p1
 portal-access-profile web1
 free-rule-template default_free_rule
 access-domain isp1 force
#
dhcp enable
#
radius-server template rd1
 radius-server shared-key cipher %^%#5Cz2!R*M%NaEr^6.]')L/$!!xTKZ<!!!!!!!!!!%^%#
 radius-server authentication 192.168.2.30 1812 weight 80
#
free-rule-template name default_free_rule
 free-rule 1 destination ip 192.168.3.31 mask 255.255.255.255
 free-rule 2 destination ip 192.168.1.1 mask 255.255.255.255
#
web-auth-server abc
 server-ip 192.168.2.30
 port 50200
 shared-key cipher %^%#'=oP;*.KKUSPqB7M5Cf2G)!!!t/&,$!!!!!!!!!!%^%#
 url http://192.168.2.30:8080/webagent
#
portal-access-profile name web1
 web-auth-server abc layer3
#
ip pool pool1
 gateway-list 10.10.10.1
 network 10.10.10.0 mask 255.255.255.0
 dns-list 192.168.2.31
#
aaa
 authentication-scheme abc
  authentication-mode radius
 domain isp1
  authentication-scheme abc
  radius-server rd1
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
 authentication-profile p1
 dhcp select global
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.1 255.255.255.0
#
ip route-static 10.10.10.0 255.255.255.0 192.168.1.2
ip route-static 192.168.2.0 255.255.255.0 192.168.2.1
#
return
```

- RouterB configuration file

```
#
sysname RouterB
#
vlan batch 10
#
dhcp enable
#
interface Vlanif10
 ip address 10.10.10.1 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 192.168.1.1
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 10
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 10
```

 Copyright © Huawei Technologies Co., Ltd. 

```
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
#
return
```

# 3.9 FAQ

## 3.9.1 When Does the 802.1x Dynamic VLAN Take Effect?

Dynamic VLAN takes effect on port-based authentication, only for access interfaces, or hybrid interface with untagged PVID.

## 3.9.2 Why Are the 802.1x Users' IP Addresses Not Displayed After I Run the Display Access-User Command?

The device learns the IP address of an authenticated online user from ARP packets that the user sends. If the user does not send any ARP packets, the device cannot learn or display the user's IP address.

## 3.9.3 Which Domain Is Preferentially Used to Authenticate Users in mac-authen Mode?

The following domains are listed in descending order of priority:

1. Domain corresponding to the MAC address that is configured by the **mac-authen domain mac-address** command in the system view
2. Domain configured by the **mac-authen domain** command in the interface view
3. Domain configured by the **mac-authen domain** command in the system view
4. Default domain in the system view

NOTE

Only V200R007 and earlier versions support this FAQ.

## 3.9.4 Which Domain Is Used Preferentially by 802.1x Users?

The following domains are listed in descending order of priority:

1. Domain that belongs to the user
2. Default domain in the system view

## 3.9.5 What Are the Functions of the Domain Configured on a WLAN-BSS Interface?

Run the **dot1x authentication domain** command, you can configure a mandatory accounting authentication domain on a WLAN-BSS interface. The domain is applied to:

 Copyright © Huawei Technologies Co., Ltd. 

1. mac-authen users for authentication and accounting
2. Non-authenticated WLAN users for accounting

NOTE

Only V200R007 and earlier versions support this FAQ.

## 3.9.6 Can MAC Bypass Authentication Be Configured on a Fixed Port on the SRU?

No, MAC bypass authentication must be configured on LPUs.

 Copyright © Huawei Technologies Co., Ltd. 

# 4 Terminal Access Configuration

## About This Chapter

4.1 Overview of BRAS Access

4.2 Configuring Terminal Access

4.3 Configuration Examples for BRAS Access

## 4.1 Overview of BRAS Access

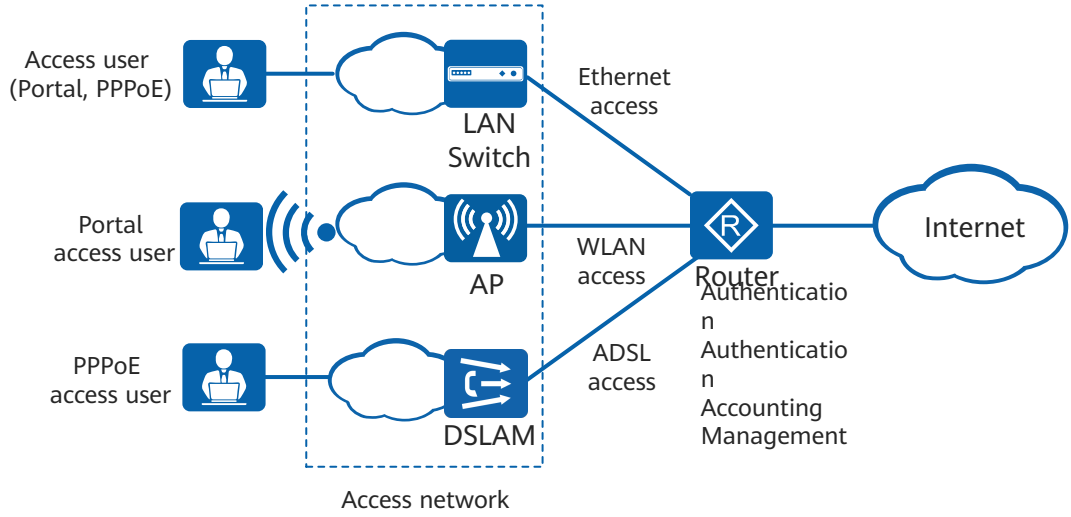
### Context

The terminal access gateway supports management of access authentication for terminal users such as PPPoE, IPoE, and L2TP terminal users. It supports access of 100 to 500 terminals of a small-sized enterprise to the NMS, and applies to scenarios of terminal address assignment and terminal user authentication.

As shown in **Figure 4-1**, the Router is the enterprise's egress gateway in the broadband network. It also acts as a terminal access to provide basic access methods and broadband access network management functions for users. The terminal access allows Ethernet access using LAN switches, WLAN access using APs, and asymmetric digital subscriber line (ADSL) access using digital subscriber line access multiplexers (DSLAMs).

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 4-1** Connecting to the Router using different broadband access modes




# 4.2 Configuring Terminal Access

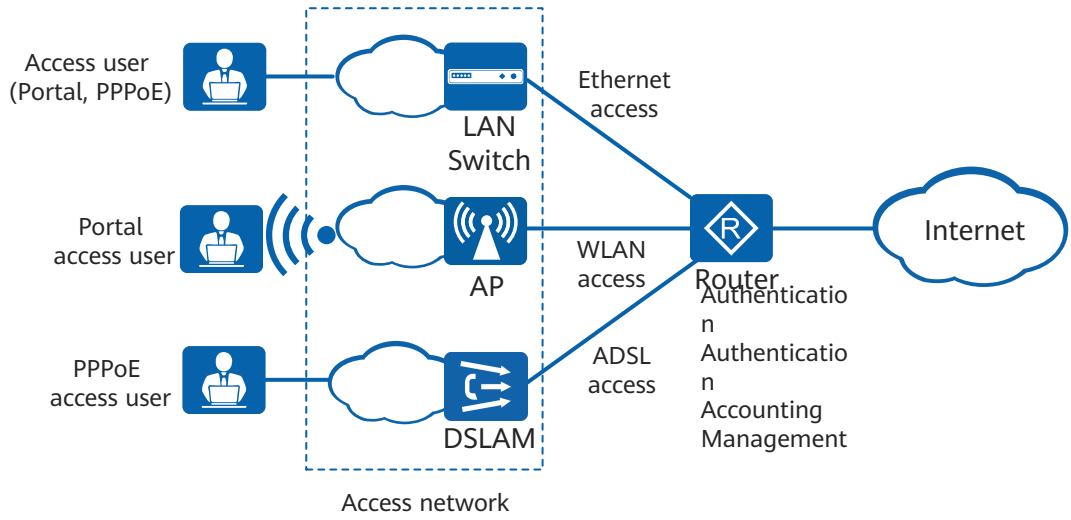
## Access User Authentication

Authentication determines whether users can access a network.

As shown in **Figure 4-2**, physical access modes of user are shielded on access devices, and the Router can identify encryption formats of user packets. That is, the terminal access differentiates users based on the protocol stacks of user packets and applies different authentication methods to users flexibly.

The Terminal access supports two authentication modes: PPPoE authentication and Portal authentication.

**Figure 4-2** Connecting to the Router using different broadband access modes

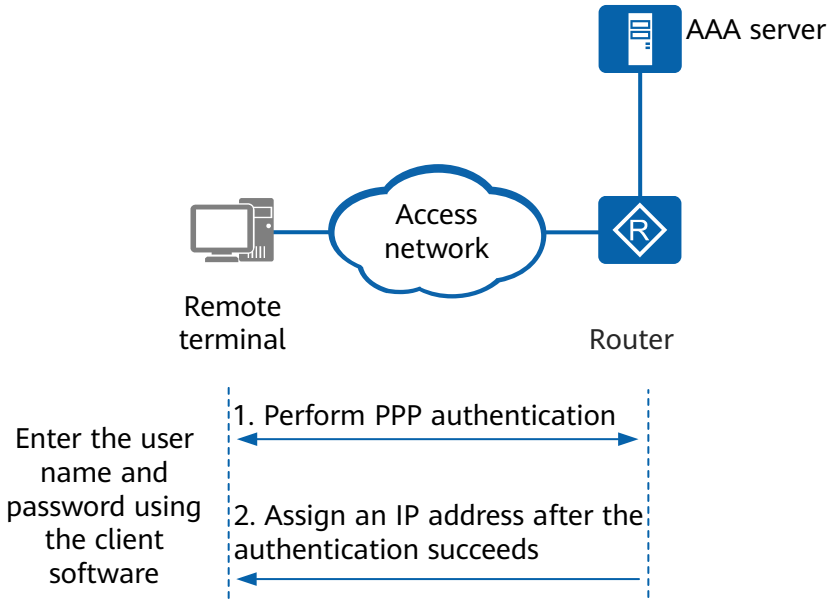



- PPPoE authentication

 Copyright © Huawei Technologies Co., Ltd. 

In **Figure 4-3**, PPPoE users connect to the Internet through PPPoE dial-up (in Ethernet or ADSL access mode). When PPPoE users use client software on their terminals to perform PPPoE dial-up, the Router functions as the PPPoE server to perform PPP authentication for the PPPoE users, and user information such as the user names and passwords are authenticated on the AAA server. After the PPPoE users are authenticated, the Router assigns IP addresses to the users so that they can access the Internet.

**Figure 4-3** PPPoE authentication process




For details on PPPoE server configuration, see Configuring the Device as a PPPoE Server in the *Huawei AR Series Access Routers Configuration Guide - WAN*.

NOTE

In addition to allocating IP addresses to PPPoE clients through the global address pool, the device can also allocate IP addresses to users through domains. That is, an IP address pool is bound to an AAA scheme and the AAA scheme is bound to a domain. When the users in the domain go online, the device allocates IP addresses to the users. The priority of IP addresses allocated through domains is higher than the priority of IP addresses allocated through the global address pool.

```
#
ip pool pool1
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 255.255.255.0
#
aaa
 service-scheme sch1
  ip-pool pool1
 domain huawei
  service-scheme sch1
#
```

- Portal authentication

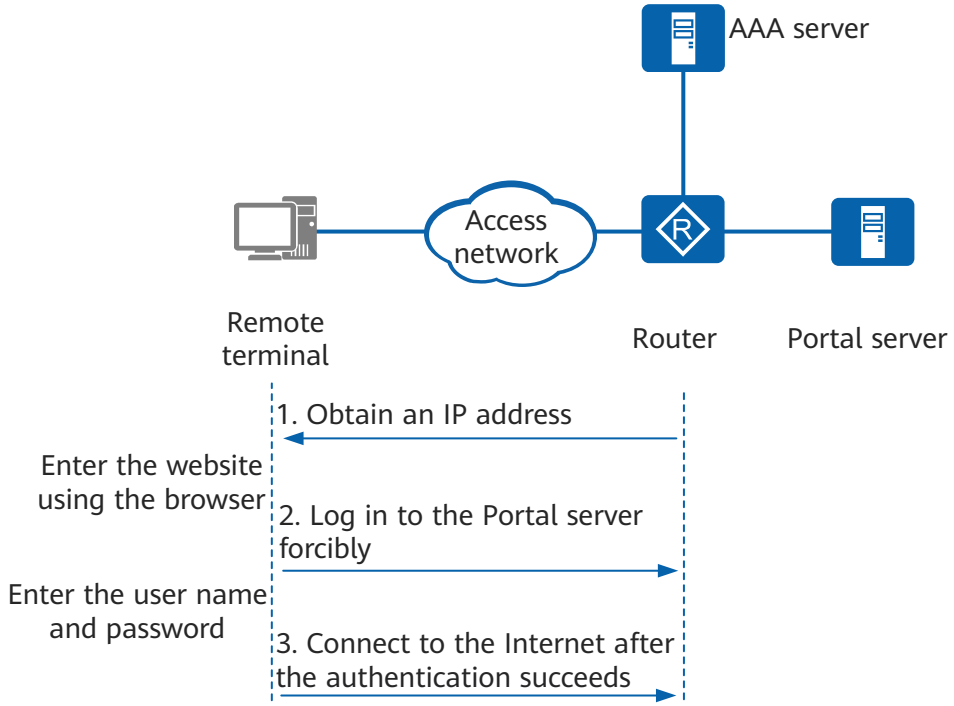
  Portal authentication (web authentication): When a user attempts to access an address before authentication, the Router redirects the access request to the forcible Portal server. The user enters the user name and password on the

 Copyright © Huawei Technologies Co., Ltd. 

authentication page. After the Router exchanges information with the remote terminal, user information such as the user name and password is authenticated on the AAA server.

In **Figure 4-4**, web users log in to the authentication page of the Portal server to access the Internet (in Ethernet or WLAN access mode). After a web user obtains a static IP address or uses DHCP to obtain an IP address, the Portal authentication website is pushed to the user for Portal authentication. The web user can access the Internet only after the authentication succeeds.

**Figure 4-4** Portal authentication process




For details on Portal authentication configuration, see **3.6 Configuring NAC** in the *Huawei AR Series Access Routers Configuration Guide - Security*.


Copyright © Huawei Technologies Co., Ltd.

NOTE

The preceding two authentication modes require AAA authentication schemes to complete user authentication. AAA is configured on the Router so that the Router can work with the AAA server. After users enter their user names and passwords, the Router receives the user authentication information and sends it to the AAA server for authentication. If the authentication succeeds, the users can access the Internet.

In Terminal access configuration, you can configure local or RADIUS authentication in an AAA authentication scheme on the Terminal access. For details on AAA authentication scheme configuration, see **1 AAA Configuration** in the *Huawei AR Series Access Routers Configuration Guide - Security*.

The Router delivers bandwidth to access users through the AAA server. Therefore, you should understand the RADIUS attributes supported by the Router. For details see **1.2.4.8 RADIUS Attributes** in the *Huawei AR Series Access Routers Configuration Guide - Security*.

In PPPoE authentication, the PPPoE server assigns IP addresses to users using the address negotiation function of the PPP protocol. In Portal authentication, static IP addresses or DHCP must be configured for users before the authentication.

- For details on how to configure static IP addresses, see IP Address Configuration in the *Huawei AR Series Access Routers Configuration Guide - IP Service*.
- For details on how to obtain IP addresses using DHCP, see DHCP Configuration in the *Huawei AR Series Access Routers Configuration Guide - IP Service*.

## User Access Management

After access users go online, the Router uses AAA to manage the users. For example, the Router charges users for the network resources they use, controls bandwidth of online users, and forces users to go offline.

- Managing access users based on domains

  In addition to authentication, AAA provides two security functions: authorization and accounting. AAA manages users based on domains, and user authentication, authorization, and accounting are all implemented in domains. All authentication, authorization, and accounting schemes for access users are created in the AAA view, and the corresponding schemes are referenced in the domain view.

  For example, users in the same domain can access the same websites and share the same accounting policies, and share the same bandwidth.

  NOTE

  Authorization information configured in a domain has a lower priority than authorization information delivered by an AAA server. That is, the authorization information delivered by an AAA server is used preferentially. When the AAA server does not have or does not support authorization, the authorization attributes configured in a domain take effect. In this manner, you can increase services flexibly by means of domain management, regardless of the authorization attributes provided by the AAA server.

- Charging access users based on their network resource usage
  - The Router performs remote accounting based on traffic or online duration through a RADIUS server.

    For the AAA accounting scheme configuration, see **1.7.2 Using RADIUS to Perform Authentication, Authorization, and Accounting** in the *Huawei AR Series Access Routers Configuration Guide - Security*.
  - Destination address accounting (DAA)

    In traffic-based accounting, if DAA is configured, users can access specified destination addresses (for example, internal network resources)

 Copyright © Huawei Technologies Co., Ltd. 

for free. When users access external networks, the Router charges the users based on the access traffic.

For the DAA configuration, see **2.7 Configuring DAA** in the *Huawei AR Series Access Routers Configuration Guide - Security*.

- Controlling access user bandwidth
  - When selecting an AAA authentication scheme in local mode:

    Create a QoS profile on the Router to specify the uplink and downlink traffic limits for each user and bind the QoS profile to the AAA service scheme. After that, access users in different domains have different bandwidths.

    i. Create a QoS profile to specify the uplink and downlink traffic limits.

    ```
    <Huawei> system-view
    [Huawei] qos-profile profile1
    [Huawei-qos-profile-profile1] car cir 200 pir 300 cbs 1500 pbs 3500 outbound
    [Huawei-qos-profile-profile1] car cir 200 pir 300 cbs 1500 pbs 3500 inbound
    [Huawei-qos-profile-profile1] quit
    ```

    ii. Create an AAA service scheme and bind the QoS profile to the scheme.

    ```
    [Huawei] aaa
    [Huawei-aaa] service-scheme scheme1
    [Huawei-aaa-service-scheme1] qos-profile profile1
    [Huawei-aaa-service-scheme1] quit
    ```

    iii. Create an AAA domain and bind the AAA service scheme to the domain.

    ```
    [Huawei-aaa] domain huawei
    [Huawei-aaa-domain-huawei] service-scheme scheme1
    ```

  - When selecting an AAA authentication scheme in RADIUS mode:

    The AAA server delivers bandwidth limits to the corresponding domains so that access users in different domains have different bandwidths.

# 4.3 Configuration Examples for BRAS Access

## 4.3.1 Example for Configuring Terminal access in Which Portal Authentication Is Used

### Networking Requirements

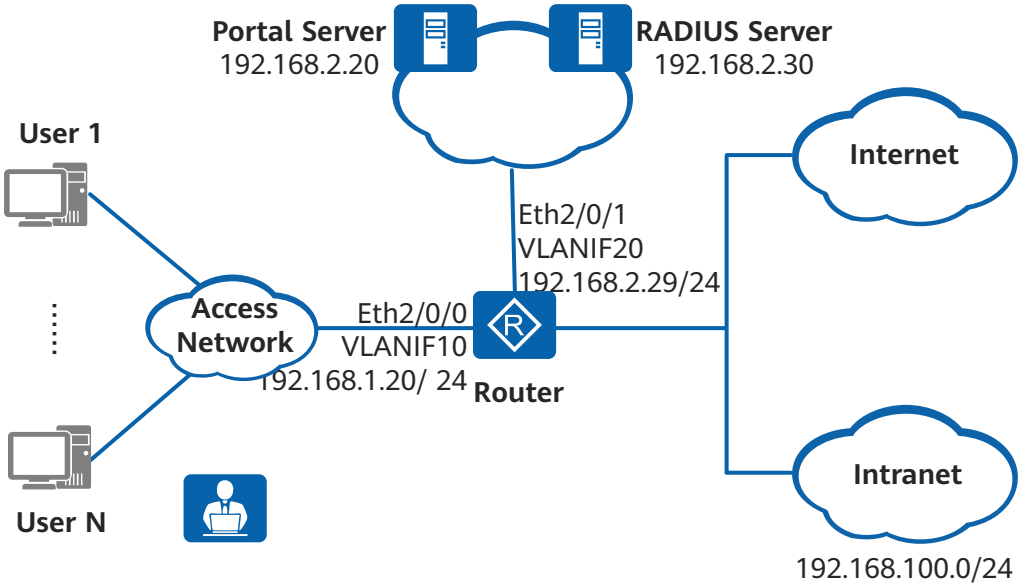
As shown in **Figure 4-5**, terminal users of an enterprise access the Internet through the Router (functioning as the egress gateway and access device). The Router needs to authenticate, charge, and manage users.

The enterprise requires that:

- Portal authentication should be used for terminal users. The Router should allow only authenticated users to access the Internet.
- The Router should not charge users for intranet (192.168.100.0/24) access, and should charge the users based on duration when they access external networks.
- If an online user is identified as an unauthorized user, the user is forced to go offline by specifying the IP address.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 4-5** Configuring terminal access in which Portal authentication is used




## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the AAA authentication and accounting schemes in RADIUS mode to ensure information exchange between the Router and RADIUS server.
2. Configure Portal authentication to authenticate access users.
3. Configure DAA. After that, the Router does not charge users for intranet (192.168.100.0/24) access, and charges the users based on duration when they access external networks.
4. Configure the device to force unauthorized users with the IP address 192.168.1.3/24 to go offline.

## Procedure

**Step 1** Create VLANs and configure interfaces to allow the VLANs to ensure network communication.

# Create VLAN 10 and VLAN 20.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10 20
```

# On the Router, configure the interface connected to users as a trunk interface and add the interface to VLAN 10.

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type trunk
[Router-Ethernet2/0/0] undo port trunk allow-pass vlan 1
[Router-Ethernet2/0/0] port trunk allow-pass vlan 10
[Router-Ethernet2/0/0] quit
```

# On the Router, configure the interface connected to the RADIUS server as a trunk interface and add the interface to VLAN 20.

```
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type trunk
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router-Ethernet2/0/1] undo port trunk allow-pass vlan 1
[Router-Ethernet2/0/1] port trunk allow-pass vlan 20
[Router-Ethernet2/0/1] quit
```

# Create VLANIF 10 and VLANIF 20, and assign IP addresses to the VLANIF interfaces so that reachable routes can be set up between the terminals, Router, and enterprise internal servers.

```
[Router] interface vlanif 10
[Router-Vlanif10] ip address 192.168.1.20 24
[Router-Vlanif10] quit
[Router] interface vlanif 20
[Router-Vlanif20] ip address 192.168.2.29 24
[Router-Vlanif20] quit
```

**Step 2** Create and configure a RADIUS server template, AAA authentication and accounting schemes, and an authentication domain.

NOTE

Ensure that the shared key in the RADIUS server template is the same as on the RADIUS server.

# Create and configure the RADIUS server template **rd1**.

```
[Router] radius-server template rd1
[Router-radius-rd1] radius-server authentication 192.168.2.30 1812
[Router-radius-rd1] radius-server accounting 192.168.2.30 1813
[Router-radius-rd1] radius-server shared-key cipher Huawei@1234
[Router-radius-rd1] quit
```

# Create an AAA scheme, configure the authentication scheme **auth**, and set the authentication mode to RADIUS authentication.

```
[Router] aaa
[Router-aaa] authentication-scheme auth
[Router-aaa-authen-auth] authentication-mode radius
[Router-aaa-authen-auth] quit
```

# Configure the accounting scheme **abc** in the AAA scheme and set the accounting mode to RADIUS accounting.

```
[Router-aaa] accounting-scheme abc
[Router-aaa-accounting-abc] accounting-mode radius
[Router-aaa-accounting-abc] quit
```

# Configure the AAA domain **isp1**, and apply the authentication scheme **auth**, accounting scheme **abc**, and RADIUS server template **rd1** to the domain.

```
[Router-aaa] domain isp1
[Router-aaa-domain-isp1] authentication-scheme auth
[Router-aaa-domain-isp1] accounting-scheme abc
[Router-aaa-domain-isp1] radius-server rd1
[Router-aaa-domain-isp1] quit
[Router-aaa] quit
```

# Configure **isp1** as the global default domain. During access authentication, enter a user name in the format user@isp1 to perform AAA authentication in the domain **isp1**. If the user name does not contain a domain name or contains an invalid domain name, the user is authenticated in the default domain.

```
[Router] domain isp1
```

**Step 3** Configure Portal authentication.

# Create and configure a Portal server template **abc**.

```
[Router] web-auth-server abc
[Router-web-auth-server-abc] server-ip 192.168.2.20
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router-web-auth-server-abc] port 50200
[Router-web-auth-server-abc] url http://192.168.2.20:8080/webagent
```

# Set the shared key that the device uses to exchange information with the Portal server to **Huawei@1234** in cipher text.

```
[Router-web-auth-server-abc] shared-key cipher Huawei@1234
```

# Configure the detection and keepalive function of Portal authentication.

```
[Router-web-auth-server-abc] server-detect action log
[Router-web-auth-server-abc] user-sync
[Router-web-auth-server-abc] quit
```

NOTE

If the Portal server does not support detection, you do not need to configure this command.

When you run the **user-sync** command, make sure that the Portal server supports this function. Otherwise, the users will go offline.

# Configure the Portal access profile web1.

```
[Router] portal-access-profile name web1
[Router-portal-access-profile-web1] web-auth-server abc direct
[Router-portal-access-profile-web1] quit
```

# Configure the authentication profile p1, bind the Portal access profile web1.

```
[Router] authentication-profile name p1
[Router-authen-profile-p1] portal-access-profile web1
[Router-authen-profile-p1] quit
```

# Bind the authentication profile p1 to VLANIF 10 and enable Portal authentication on the interface.

```
[Router] interface vlanif 10
[Router-Vlanif10] authentication-profile p1
[Router-Vlanif10] quit
```

**Step 4** Configure DAA.

# Configure the traffic identification rule ACL 3000 to identify the traffic destined for the internal network segment 192.168.100.0/24.

```
[Router] acl 3000
[Router-acl-adv-3000] rule 5 permit ip destination 192.168.100.0 0.0.0.255
[Router-acl-adv-3000] quit
```

# Set the tariff level for access the internal network to 1.

```
[Router] traffic-group huawei
[Router-traffic-group-huawei] acl 3000 tariff-level 1
[Router-traffic-group-huawei] quit
[Router] traffic-group huawei enable
```

# Configure accounting for all the traffic that does not match ACL 3000.

- For traffic of tariff level 1, traffic statistics collection is disabled and accounting is not performed.
- For other traffic, the device collects traffic statistics and sends the statistics to the RADIUS accounting server.

```
[Router] aaa
[Router-aaa] domain isp1
[Router-aaa-domain-isp1] statistic enable
[Router-aaa-domain-isp1] quit
```

 Copyright © Huawei Technologies Co., Ltd. 

**Step 5** Force the access users with the IP address 192.168.1.3 to go offline.

```
[Router-aaa] cut access-user ip-address 192.168.1.3
[Router-aaa] quit
[Router] quit
```

**Step 6** Verify the configuration.

# Run the **display web-auth-server configuration** command to check the configuration of the Portal server.

```
<Router> display web-auth-server configuration
  Listening port        : 2000
  Portal                : version 1, version 2
  Include reply message : enabled

------------------------------------------------------------------------------
  Web-auth-server Name : abc
  IP-address           : 192.168.2.20
  Shared-key           : %^%#s@<60z+%'"EJI#4KOij5M)"m&9%"k:63Vl+xTc"K%^%#
  Source-IP            : -
  Port / PortFlag      : 50200 / NO
  URL                  : http://192.168.2.20:8080/webagent
  URL Template         :
  Redirection          : Enable
  Sync                 : Enable
  Sync Seconds         : 300
  Sync Max-times       : 3
  Detect               : Enable
  Detect Seconds       : 60
  Detect Max-times     : 3
  Detect Critical-num  : 0
  Detect Action        : log
  Bound Vlanif         : 10
  VPN Instance         :
  Bound Interface      :


------------------------------------------------------------------------------
  1 Web authentication server(s) in total
```

Run the **display traffic-group name** command to check information about the traffic group **huawei**.

```
<Router> display traffic-group name huawei
  ------------------------------------------------------------------------------
  Acl-id               Tariff-level
  ------------------------------------------------------------------------------
  3000                    1
  ------------------------------------------------------------------------------
  Total: 1
```

# After the user goes online, run the **display access-user** command to check traffic statistics at each tariff level.

**----End**

## Configuration Files

Configuration files on Router

```
#
 sysname Router
#
vlan batch 10 20
#
authentication-profile name p1
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 portal-access-profile web1
#
domain isp1
#
radius-server template rd1
 radius-server shared-key cipher %^%#s@<60z+%'"EJI#4KOij5M)"m&9%"k:63Vl+xTc"K%^%#
 radius-server authentication 192.168.2.30 1812 weight 80
 radius-server accounting 192.168.2.30 1813 weight 80
#
acl number 3000
 rule 5 permit ip destination 192.168.100.0 0.0.0.255
#
web-auth-server abc
 server-ip 192.168.2.20
 port 50200
 shared-key cipher %^%#s@<60z+%'"EJI#4KOij5M)"m&9%"k:63Vl+xTc"K%^%#
 url http://192.168.2.20:8080/webagent

server-detect action log
 user-sync
#
portal-access-profile name web1
 web-auth-server abc direct
#
aaa
 authentication-scheme auth
  authentication-mode radius
 accounting-scheme abc
  accounting-mode radius
 domain isp1
  authentication-scheme auth
  accounting-scheme abc
  radius-server rd1
  statistic enable
#
interface Vlanif10
 ip address 192.168.1.20 255.255.255.0
 authentication-profile p1
#
interface Vlanif20
 ip address 192.168.2.29 255.255.255.0
#
interface Ethernet2/0/0
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
interface Ethernet2/0/1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 20
#
traffic-group huawei
  acl 3000 tariff-level 1
traffic-group huawei enable
#
return
```

## 4.3.2 Example for Configuring Terminal access in Which PPPoE Authentication Is Used

### Networking Requirements

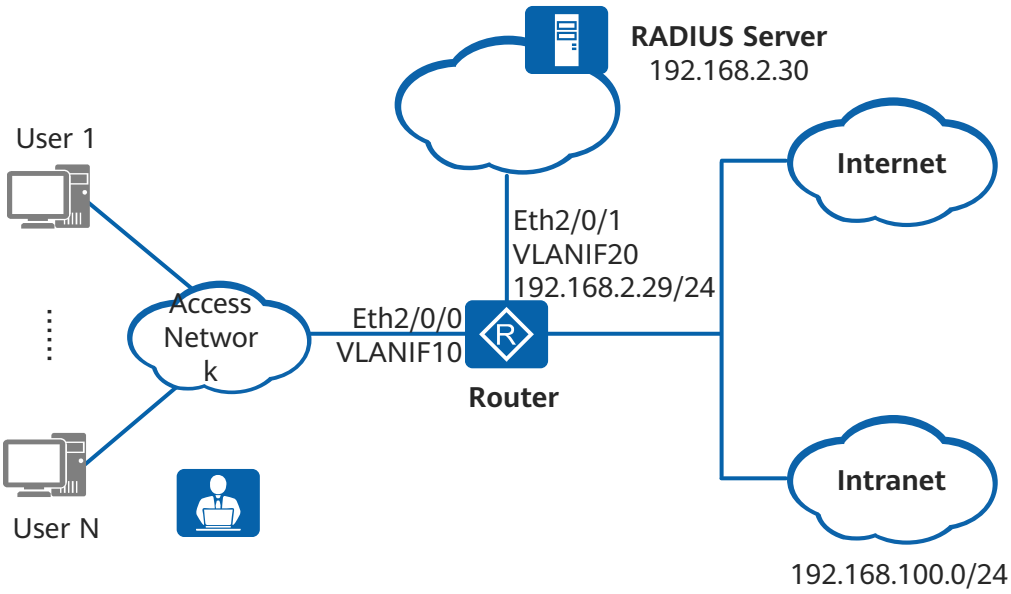
As shown in **Figure 4-6**, terminal users of an enterprise access the Internet through the Router (functioning as the egress gateway and access device). The Router needs to authenticate, charge, and manage users.

 Copyright © Huawei Technologies Co., Ltd. 

The enterprise requires that:

- PPPoE authentication should be used for terminal users. The Router should allow only authenticated users to access the Internet.
- The Router should not charge users for intranet (192.168.100.0/24) access, and should charge the users based on duration when they access external networks.
- If an online user is identified as an unauthorized user, the user is forced to go offline by specifying the IP address.

**Figure 4-6** Configuring terminal access in which PPPoE authentication is used




## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the AAA authentication and accounting schemes in RADIUS mode to ensure information exchange between the Router and RADIUS server.
2. Configure the PPPoE server to perform PPP authentication on access users.
3. Configure DAA. After that, the Router does not charge users for intranet access, and charges the users based on duration when they access external networks.
4. Configure the device to force unauthorized users with the IP address 192.168.1.3/24 to go offline.

## Procedure

**Step 1** Create VLANs and configure interfaces to allow the VLANs to ensure network communication.

# Create VLAN 10 and VLAN 20.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10 20
```

# On the Router, configure the interface connected to users as a trunk interface and add the interface to VLAN 10.

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type trunk
[Router-Ethernet2/0/0] undo port trunk allow-pass vlan 1
[Router-Ethernet2/0/0] port trunk allow-pass vlan 10
[Router-Ethernet2/0/0] quit
```

# On the Router, configure the interface connected to the RADIUS server as a trunk interface and add the interface to VLAN 20.

```
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type trunk
[Router-Ethernet2/0/1] undo port trunk allow-pass vlan 1
[Router-Ethernet2/0/1] port trunk allow-pass vlan 20
[Router-Ethernet2/0/1] quit
```

# Create VLANIF 10 and VLANIF 20, and assign IP address to the VLANIF20 interface so that reachable routes can be set up between the terminals, Router, and enterprise internal servers.

```
[Router] interface vlanif 10
[Router-Vlanif10] quit
[Router] interface vlanif 20
[Router-Vlanif20] ip address 192.168.2.29 24
[Router-Vlanif20] quit
```

**Step 2** Create and configure a RADIUS server template, an AAA authentication scheme, accounting scheme and an authentication domain.

NOTE

Ensure that the shared key in the RADIUS server template is the same as on the RADIUS server.

# Create and configure the RADIUS server template **rd1**.

```
[Router] radius-server template rd1
[Router-radius-rd1] radius-server authentication 192.168.2.30 1812
[Router-radius-rd1] radius-server accounting 192.168.2.30 1813
[Router-radius-rd1] radius-server shared-key cipher Huawei@1234
[Router-radius-rd1] quit
```

# Create an AAA scheme, configure the authentication scheme **auth**, and set the authentication mode to RADIUS authentication.

```
[Router] aaa
[Router-aaa] authentication-scheme auth
[Router-aaa-authen-auth] authentication-mode radius
[Router-aaa-authen-auth] quit
```

# Configure the accounting scheme **abc** in the AAA scheme and set the accounting mode to RADIUS accounting.

```
[Router-aaa] accounting-scheme abc
[Router-aaa-accounting-abc] accounting-mode radius
[Router-aaa-accounting-abc] quit
```

# Configure the AAA domain **isp1**, and apply the authentication scheme **auth**, accounting scheme **abc**, and RADIUS server template **rd1** to the domain.

```
[Router-aaa] domain isp1
[Router-aaa-domain-isp1] authentication-scheme auth
[Router-aaa-domain-isp1] accounting-scheme abc
[Router-aaa-domain-isp1] radius-server rd1
[Router-aaa-domain-isp1] quit
[Router-aaa] quit
```

 Copyright © Huawei Technologies Co., Ltd. 

# Configure **isp1** as the global default domain. During access authentication, enter a user name in the format user@isp1 to perform AAA authentication in the domain **isp1**. If the user name does not contain a domain name or contains an invalid domain name, the user is authenticated in the default domain.

```
[Router] domain isp1
```

**Step 3** Configure the PPPoE server.

# Configure a global address pool so that the PPPoE server can dynamically assign IP addresses to access users.

```
[Router] ip pool pool1
[Router-ip-pool-pool1] network 192.168.1.0 mask 255.255.255.0
[Router-ip-pool-pool1] gateway-list 192.168.1.1
[Router-ip-pool-pool1] quit
```

# Create and configure a virtual interface template.

```
[Router] interface virtual-template 1
[Router-Virtual-Template1] ppp authentication-mode chap domain isp1
[Router-Virtual-Template1] ip address 192.168.1.1 255.255.255.0
[Router-Virtual-Template1] remote address pool pool1
[Router-Virtual-Template1] quit
```

# Enable the PPPoE protocol on the VLANIF10 interface.

```
[Router] interface vlanif10
[Router-Vlanif10] pppoe-server bind virtual-template 1
[Router-Vlanif10] quit
```

**Step 4** Configure DAA.

# Configure the traffic identification rule ACL 3000 to identify the traffic destined for the internal network segment 192.168.100.0/24.

```
[Router] acl 3000
[Router-acl-adv-3000] rule 5 permit ip destination 192.168.100.0 0.0.0.255
[Router-acl-adv-3000] quit
```

# Set the tariff level to 1.

```
[Router] traffic-group huawei
[Router-traffic-group-huawei] acl 3000 tariff-level 1
[Router-traffic-group-huawei] quit
[Router] traffic-group huawei enable
```

# Configure accounting for all the traffic that does not match ACL 3000.

- For traffic of tariff level 1, traffic statistics collection is disabled and accounting is not performed.
- For other traffic, the device collects traffic statistics and sends the statistics to the RADIUS accounting server.

```
[Router] aaa
[Router-aaa] domain isp1
[Router-aaa-domain-isp1] statistic enable
[Router-aaa-domain-isp1] quit
```

**Step 5** Force the access users with the IP address 192.168.1.3 to go offline.

```
[Router-aaa] cut access-user ip-address 192.168.1.3
[Router-aaa] quit
[Router] quit
```

**Step 6** Verify the configuration.

 Copyright © Huawei Technologies Co., Ltd. 

# Run the **display pppoe-server session all** command to check the PPPoE session status and configuration. The command output shows that the PPPoE session status is Up and the session configuration is correct.

Run the **display traffic-group name** command to check information about the traffic group **huawei**.

```
<Router> display traffic-group name huawei
 --------------------------------------------------------------------------------
 Acl-id              Tariff-level
 --------------------------------------------------------------------------------
 3000                   1
 --------------------------------------------------------------------------------
 Total: 1
```

# After the user goes online, run the **display access-user** command to check the IP address and traffic statistics of online users.

**----End**

## Configuration Files

Configuration files on Router

```
#
 sysname Router
#
vlan batch 10 20
#
domain isp1
#
radius-server template rd1
 radius-server shared-key cipher %#%#s@<60z+%'"EJI#4KOij5M)"m&9%"k:63Vl+xTc"K%#%#
 radius-server authentication 192.168.2.30 1812 weight 80
 radius-server accounting 192.168.2.30 1813 weight 80
#
acl number 3000
 rule 5 permit ip destination 192.168.100.0 0.0.0.255
#
ip pool pool1
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 255.255.255.0
#
aaa
 authentication-scheme auth
  authentication-mode radius
 accounting-scheme abc
  accounting-mode radius
 domain isp1
  authentication-scheme auth
  accounting-scheme abc
  radius-server rd1
  statistic enable
#
interface Vlanif10
 pppoe-server bind Virtual-Template 1
#
interface Vlanif20
 ip address 192.168.2.29 255.255.255.0
#
interface Ethernet2/0/0
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
interface Ethernet2/0/1
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 20
#
interface Virtual-Template1
 ppp authentication-mode chap domain isp1
 remote address pool pool1
 ip address 192.168.1.1 255.255.255.0
#
traffic-group huawei
  acl 3000 tariff-level 1
traffic-group huawei enable
#
return
```

# 5 ACL Configuration

## About This Chapter

An Access Control List (ACL) is a set of rules that classify packets into different types. This chapter explains how to configure an ACL on a Router to filter packets.

5.1 Overview of ACLs

5.2 Understanding ACLs

5.3 Application Scenarios for ACLs

5.4 Summary of ACL Configuration Tasks

5.5 Licensing Requirements and Limitations for ACLs

5.6 Default Settings for ACLs

5.7 Configuring ACLs

5.8 Maintaining ACLs

5.9 Configuration Examples for ACLs

5.10 Troubleshooting ACLs

5.11 FAQ About ACLs

## 5.1 Overview of ACLs

### Definition

An Access Control List (ACL) is a packet filter that filters packets based on rules. One or more rules describe the packet matching conditions, such as the source address, destination address, and port number of packets.

For packets that match the ACL rules configured on a device, the device forwards or discards these packets according to the policies used by the service module to which the ACL is applied.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

A configured ACL takes effect only after it is applied to a service module.

An ACL can be applied to various service modules, such as Telnet, FTP, and routing. Usually, an ACL is applied to a traffic policy or simplified traffic policy so that the device can deliver ACL rules globally, in a VLAN, or on an interface to filter packets to be forwarded. The service modules use different actions and mechanisms to process the packets filtered by ACL. For details, see **5.2.7 Default ACL Actions and Mechanisms of Different Service Modules**.

## Purpose

The fast growth of network technologies brings challenges to network security and Quality of Service (QoS). ACL is a security policy that is enforced on networks to prevent the following problems:

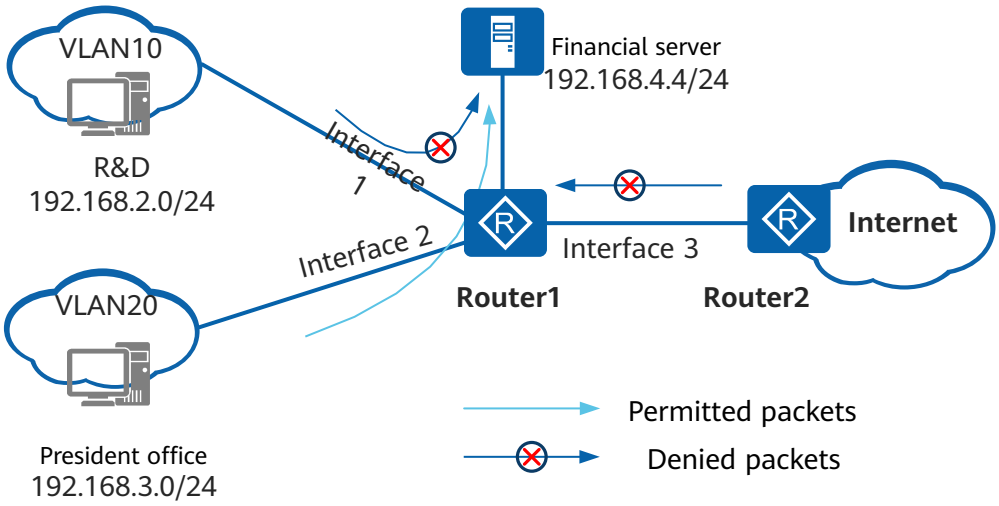
- To prevent information leaks and unauthorized access of resources on key servers of an enterprise network
- To prevent viruses on the Internet from entering and spreading on the enterprise intranet
- To prevent random services from occupying network bandwidth, thereby guaranteeing bandwidth for delay-sensitive services such as voice and video

These problems are detrimental to network communication, so network security is critical.

ACL accurately identifies and controls packets on the network to manage network access behaviors, prevent network attacks, and improve bandwidth use efficiency. In this way, ACL ensures security and high service quality on networks.

**Figure 5-1** shows a typical network with ACL configured.

**Figure 5-1** ACL application scenario




- To ensure financial data security, access to the financial server is allowed only from the president office; access from the R&D department to the financial server is blocked. The implementation method is as follows:

  Configure an ACL in the inbound direction of Interface 1 to block the packets from the R&D department to the financial server. The ACL does not need to

 Copyright © Huawei Technologies Co., Ltd. 

be configured on Interface 2, so the packets from the president office to the financial server are allowed.

- Protect the enterprise intranet against viruses entering and spreading from the Internet. The implementation method is as follows:

  Configure an ACL on Interface 3 to block packets that match virus signatures.

# 5.2 Understanding ACLs

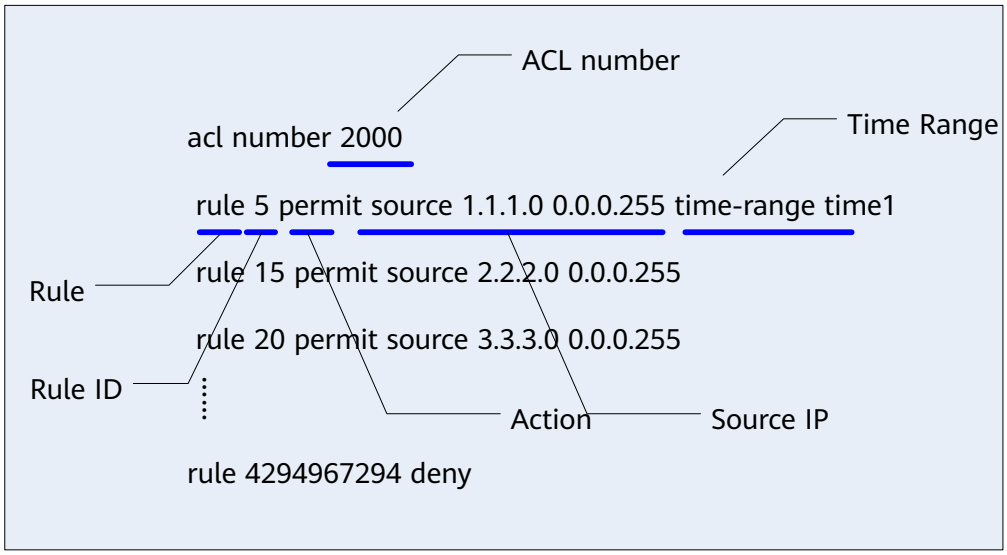
## 5.2.1 ACL Fundamentals

An ACL matches packets against the rules in contains to filter packets.

### ACL Structure

**Figure 5-2** shows the structure of an ACL.

**Figure 5-2** ACL structure




- **ACL number**: identifies a numbered ACL.

  ACLs are classified into basic ACL, advanced ACL, Layer 2 ACL, user ACL. These ACLs have different number ranges. For details, see **5.2.2 ACL Classification**.

  You can also define the name of an ACL to help you remember the ACL's purpose. In this situation, an ACL name is like a domain name that represents an IP address. Such an ACL is called named ACL.

  An ACL number can be part of an ACL name. That is, you can also specify an ACL number when you define an ACL name. If you do not specify an ACL number, the system will automatically allocate a number to an ACL. The following is an ACL name consisting of a name **deny-telnet-login** and a number **3998**.

  ```
  #
  acl name deny-telnet-login 3998
  ```


Copyright © Huawei Technologies Co., Ltd.

```
 rule 0 deny tcp source 10.152.0.0 0.0.63.255 destination 10.64.0.97 0 destination-port eq
telnet
 rule 5 deny tcp source 10.242.128.0 0.0.127.255 destination 10.64.0.97 0 destination-port eq
telnet
#
```

- **Rule**: describes packet matching conditions.
  - **Rule ID**: identifies an ACL rule. The rule IDs can be manually set or automatically allocated by the system.

    The ACL rule IDs range from 0 to 4294967294. The rule IDs in an ACL are allocated in an ascending order. Therefore, in **Figure 5-2**, rule 5 is in the first line and rule 4294967294 is in the bottom line of an ACL. The system matches packets against the rules from the first line to the bottom line, and stops matching if the packets match a rule.
  - **Action**: includes permit and deny.
  - **Matching option**: ACLs support many matching conditions, including Layer 2 Ethernet frame header information (source MAC, destination MAC, and Ethernet protocol type), Layer 3 packet information (destination address and protocol type), and Layer 4 packet information (TCP/UDP port number). For details about ACL matching conditions, see **5.2.5 Matching Conditions**.

  NOTE

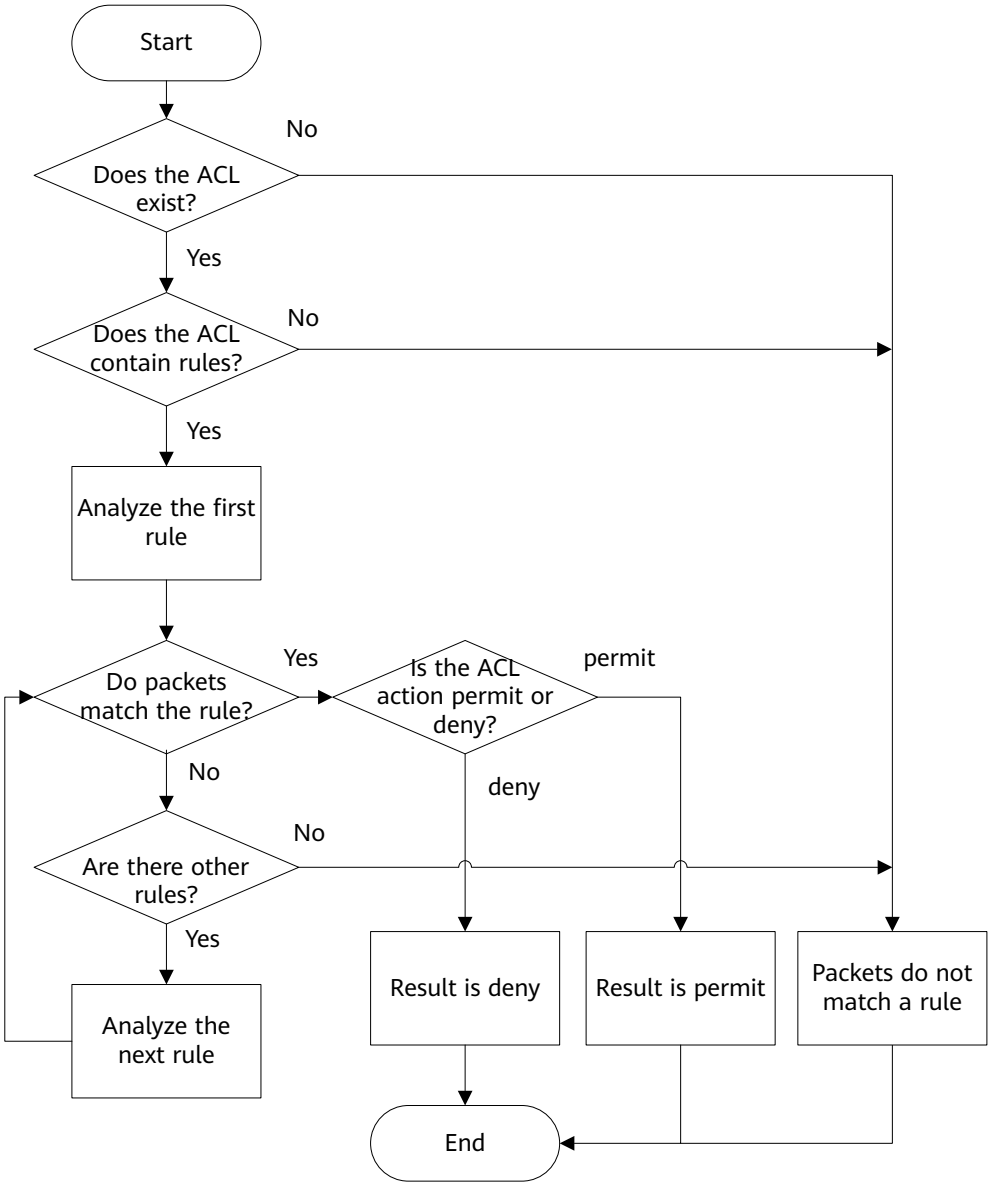
  If the ACL rules with the numbers beyond the acceptable range are set in the configuration file used for startup, the ACL configuration can be generated when the device starts, but some configurations do not take effect.

## Matching Mechanism

The device stops matching packets against ACL rules as long as the packets match one rule, as shown in **Figure 5-3**.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 5-3** ACL matching mechanism




The device checks whether an ACL is configured.

- If no ACL is configured, the device returns the result "negative match."
- If an ACL is configured, the device checks whether the ACL contains rules.
  - If the ACL does not contain rules, the device returns the result "negative match."
  - If the ACL contains rules, the device matches the packets against the rules in ascending order of rule IDs.
    - When the packets match a permit rule, the device stops matching and returns the result "positive match (permit)."
    - When the packets match a deny rule, the device stops matching and returns the result "positive match (deny)."

 Copyright © Huawei Technologies Co., Ltd. 

    - If the packets do not match any rule in the ACL, the device returns the result "negative match."

The ACL matching results include "positive match" and "negative match."

- Positive match: Packets match a rule in an ACL.

  The result is "positive match" regardless of whether packets match a permit or deny rule in an ACL.
- Negative match: No ACL exists, the ACL does not contain rules, or packets do not match any rule in an ACL.

NOTE

Different service modules process the packets that match and do not match ACL rules in different ways. For example, the Telnet module forwards the packets matching the permit rules, whereas the traffic policy module discards the packets matching the permit rule if the action configured in the traffic policy module is deny. For details about ACL processing in each service module, see **5.2.7 Default ACL Actions and Mechanisms of Different Service Modules**.

# 5.2.2 ACL Classification

## Based on ACL Naming Methods

ACLs are classified into:

- Numbered ACL: This is the traditional naming method. After an ACL is created, a unique number is specified for the ACL.
- Named ACL: An ACL is identified by a name.

You can specify a number for a created ACL. Different types of ACLs have different number ranges, as described in **Table 5-1**. You can also specify a name for the created ACL to help you remember the ACL's purpose. A named ACL consists of a name and number. That is, you can specify an ACL number when you define an ACL name. If you do not specify a number for a numbered ACL, the device automatically allocates a number to it.

NOTE

The name of a named ACL cannot be modified. Deleting an ACL name will delete the ACL.

Repeated ACL names can only be used between basic ACL and basic ACL6, and between advanced ACL and advanced ACL6.

## Based on IP Protocol Versions

ACLs are classified into:

- ACL4: filters IPv4 packets. It is also called ACL.
- ACL6: filters IPv6 packets. It is also called IPv6 ACL.

In this document, ACL refers to ACL4, ACL6, and the ACL supporting both IPv4 and IPv6 packet filtering. **Table 5-1** describes how each type of ACLs supports IPv4 and IPv6 packets.

 Copyright © Huawei Technologies Co., Ltd. 

### Based on ACL Rule Definition Methods

Table 5-1 describes the ACLs based on rule definition methods.

**Table 5-1** ACL classification based on ACL rule definition methods

| Category | IP Version | Rule Definition Description | Number Range |
| --- | --- | --- | --- |
| Basic ACL | IPv4 | Defines rules based on **source IP addresses**, fragmentation information, and time ranges. | 2000-2999 |
| Advanced ACL | IPv4 | Defines rules based on **source IPv4 addresses**, **destination IPv4 addresses**, IPv4 protocol types, ICMP types, TCP source/destination port numbers, UDP source/destination port numbers, and time ranges. | 3000-3999 |
| Layer 2 ACL | IPv4&IPv6 | Defines rules based on **information in Ethernet frame headers** of packets, such as the source MAC addresses, destination MAC addresses, and Layer 2 protocol types. | 4000-4999 |
| User ACL | IPv4 | Defines rules based on **source IPv4 addresses**/**destination IPv4 addresses**, IPv4 protocol types, ICMP types, TCP source/destination port numbers, and UDP source/destination port numbers. | 6000-6031 |
| Basic ACL6 | IPv6 | Defines rules based on **source IPv6 addresses**, fragmentation information, and time ranges. | 2000-2999 |
| Advanced ACL6 | IPv6 | Defines rules based on **source IPv6 addresses**, **destination IPv6 addresses**, IPv6 protocol types, ICMPv6 types, TCP source/destination port numbers, UDP source/destination ports, and time ranges. | 3000-3999 |

## 5.2.3 Step


Copyright © Huawei Technologies Co., Ltd.

## What Is a Step

A step is an increment between neighboring rule IDs automatically allocated by the system.

If a rule is added to an empty ACL without a rule ID manually specified, the system allocates the step value as the ID to this rule. If an ACL contains rules with manually configured IDs and a new rule is added without an ID manually configured, the system allocates to this new rule the minimum multiple of the step value which is greater than the largest rule ID in the ACL. Rule IDs must be integers. For example, an ACL (basic ACL, advanced ACL, Layer 2 ACL, user ACL) contains rule 5 and rule 12, and the default step is 5. When a new rule is added to the ACL, the system allocates ID 15 to this new rule (15 is greater than 12 and is the minimum multiple of 5).

```
[Huawei-acl-basic-2001] display this
#
acl number 2001              //Empty ACL
#
return
[Huawei-acl-basic-2001] rule deny source 10.1.1.0 0.0.0.255 //Configure the first rule without specifying an ID.
[Huawei-acl-basic-2001] display this
#
acl number 2001
 rule 5 deny source 10.1.1.0 0.0.0.255
#
return
[Huawei-acl-basic-2001] rule 12 deny source 10.2.2.0 0.0.0.255 //Configure a rule with ID 12.
[Huawei-acl-basic-2001] display this
#
acl number 2001
 rule 5 deny source 10.1.1.0 0.0.0.255
 rule 12 deny source 10.2.2.0 0.0.0.255
#
return
[Huawei-acl-basic-2001] rule deny source 10.3.3.0 0.0.0.255 //Configure another rule without specifying an ID.
[Huawei-acl-basic-2001] display this
#
acl number 2001
 rule 5 deny source 10.1.1.0 0.0.0.255
 rule 12 deny source 10.2.2.0 0.0.0.255
 rule 15 deny source 10.3.3.0 0.0.0.255
#
return
```

If the step value of an ACL is changed, the system reallocates IDs to rules in the ACL. For example, when the step value is changed to 2, the system allocates 2, 4, 6... to rules. After the step is restored to the default value, the system reallocates IDs to the rules using the default step, that is, 5, 10, 15....

```
[Huawei-acl-basic-2001] display acl 2001
Basic ACL 2001, 3 rules
Acl's step is 5
 rule 5 deny source 10.1.1.0 0.0.0.255
 rule 12 deny source 10.2.2.0 0.0.0.255
 rule 15 deny source 10.3.3.0 0.0.0.255

[Huawei-acl-basic-2001] step 2   //Set the step to 2
[Huawei-acl-basic-2001] display acl 2001
Basic ACL 2001, 3 rules
Acl's step is 2
 rule 2 deny source 10.1.1.0 0.0.0.255
 rule 4 deny source 10.2.2.0 0.0.0.255
 rule 6 deny source 10.3.3.0 0.0.0.255
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Huawei-acl-basic-2001] undo step   //Restore the default step.
[Huawei-acl-basic-2001] display acl 2001
Basic ACL 2001, 3 rules
Acl's step is 5
 rule 5 deny source 10.1.1.0 0.0.0.255
 rule 10 deny source 10.2.2.0 0.0.0.255
 rule 15 deny source 10.3.3.0 0.0.0.255
```

### How a Step Functions

Setting a step facilitates rule insertion between existing rules of an ACL.

For example, an ACL contains rule 5, rule 10, and rule 15. The network administrator wants to add a rule that denies the packets from source IP address 10.1.1.3. The rules are as follows:

```
rule 5 deny source 10.1.1.1 0  //Reject the packets from source IP address 10.1.1.1.
rule 10 deny source 10.1.1.2 0 //Reject the packets from source IP address 10.1.1.2.
rule 15 permit source 10.1.1.0 0.0.0.255 //Reject the packets from source IP address segment 10.1.1.0/24.
```

The system stops matching packets once the packets matching a rule. Therefore, the packets from source addresses 10.1.1.1 and 10.1.1.2 match rule 5 and rule 10, and are discarded; the packets from source address 10.1.1.3 match rule 15, and are forwarded. To deny the packets from source IP address 10.1.1.3, add a new deny rule. You can add rule 11 before rule 15 so that the packets from source IP address 10.1.1.3 match rule 11 and are discarded. Rule 11 does not affect existing rule IDs in the ACL. The rule IDs are 5, 10, 11, and 15.

```
rule 5 deny source 10.1.1.1 0  //Reject the packets from source IP address 10.1.1.1.
rule 10 deny source 10.1.1.2 0 //Reject the packets from source IP address 10.1.1.2.
rule 11 deny source 10.1.1.3 0 //Reject the packets from source IP address 10.1.1.3.
rule 15 permit source 10.1.1.0 0.0.0.255 //Reject the packets from source IP address segment 10.1.1.0.
```

To add a rule to an ACL with the step value of 1 (rule 1, rule 2, rule 3...), you must delete existing rules, add the new rule, and then reconfigure the deleted rules.

A step resolves the preceding issue and facilitates rule insertion.

## 5.2.4 Matching Order

An ACL consists of multiple deny | permit clauses, each of which describes a rule. These rules may repeat or conflict. For example, an ACL contains two rules:

```
rule deny ip destination 10.1.0.0 0.0.255.255   //Reject the packets destined for network segment 10.1.0.0/16.
rule permit ip destination 10.1.1.0 0.0.0.255   //Permit the packets destined for network segment
10.1.1.0/24, which has a smaller range than 10.1.0.0/16.
```

The permit and deny rules conflict. If the system first matches a packet destined for 10.1.1.1 against the deny rule, the packet is discarded. However, if the system matches the packet against the permit rule first, the packet is forwarded.

Therefore, if ACL rules repeat or conflict, the matching order decides the matching result.

The device supports two matching orders: the configuration order (**config**) and the automatic order (**auto**). The default order is **config**.

 Copyright © Huawei Technologies Co., Ltd. 

## Config Order

The system matches packets against ACL rules in ascending order of rule IDs. That is, the rule with the smallest ID is processed first.

- If a smaller rule ID is manually specified for a rule, the rule is inserted in one of the front lines of an ACL, and the rule is processed earlier.
- If no ID is manually specified for a rule, the system allocates an ID to the rule. The rule ID is greater than the largest rule ID in the ACL and is the minimum multiple of the step; therefore, this rule is processed last.

## Auto Order

The system arranges rules according to the precision degree of the rules (depth first principle), and matches packets against the rules in descending order of precision. A rule with the highest precision defines strictest conditions, and has the highest priority. The system matches packets against this rule first. **Table 5-2** describes how the auto order is applied to each type of ACL.

For details about the ACL matching conditions mentioned in **Table 5-2**, such as IP address wildcard mask, types of protocols carried by IP, TCP/UDP ports, Layer 2 protocol type wildcard mask, and MAC address wildcard mask, see **5.2.5 Matching Conditions**.

**Table 5-2** Auto matching order

| ACL Type | Matching Rules |
| --- | --- |
| Basic ACL and basic ACL6 | 1. The rule that defines a VPN instance is processed first.<br>2. The rule that defines the smallest source IP address range is processed. The wildcard mask with the most 0 bits identifies the smallest source IP address range.<br>3. If the source IP address ranges are the same, the rule with the smallest ID is processed. |
| Advanced ACL and advanced ACL6 | 1. The rule that defines a VPN instance is processed first.<br>2. The rule that defines a protocol type is processed.<br>3. If the protocol types are the same, the rule that defines the smallest source IP address range is processed. The wildcard mask with the most 0 bits identifies the smallest source IP address range.<br>4. If the protocol types and source IP address ranges are the same, the rule that defines the smallest destination IP address range is processed. The wildcard mask with the most 0 bits identifies the smallest destination IP address range.<br>5. If the protocol types, source IP address ranges, and destination IP address ranges are the same, the rule that defines the smallest Layer 4 port number (TCP/UDP port number) range is processed.<br>6. If the preceding ranges are all the same, the rule with the smallest ID is processed. |

 Copyright © Huawei Technologies Co., Ltd. 

| ACL Type | Matching Rules |
| --- | --- |
| Layer 2 ACL | 1. The rule with the largest L2 protocol type wildcard (with the most 1 bits in the wildcard mask) is processed first.<br>2. The rule that defines the smallest source MAC address range is processed. The wildcard mask with the most 1 bits identifies the smallest source MAC address range.<br>3. If the source MAC address ranges are the same, the rule that defines the smallest destination MAC address range is processed. The wildcard mask with the most 1 bits identifies the smallest destination MAC address range.<br>4. If the source and destination MAC address ranges are the same, the rule with the smallest ID is processed. |
| User ACL | 1. The rule that defines a protocol type is processed first.<br>2. If the protocol types are the same, the source IP address ranges are compared. If all source IP addresses are IP network segments, the rule with a smaller source IP address (with more 0 bits in wildcard mask) is processed.<br>3. If the protocol types and source IP address ranges are the same, the destination IP address ranges are compared. If all destination IP addresses are IP network segments, the rule with a smaller destination IP address (with more 0 bits in wildcard mask) is processed.<br>4. If the protocol types, source IP address ranges, and destination IP address ranges are the same, the rule that defines the smallest Layer 4 port number (TCP/UDP port number) range is processed.<br>5. If the preceding ranges are all the same, the rule with the smallest ID is processed. |

If you add a rule to an ACL in auto mode, the system automatically identifies the rule priority and assigns an ID to the rule.

For example, two rules are added to advanced ACL 3001 in auto mode:

```
rule deny ip destination 10.1.0.0 0.0.255.255   //Reject the packets destined for network segment 10.1.0.0/16.
rule permit ip destination 10.1.1.0 0.0.0.255   //Permit the packets destined for network segment
10.1.1.0/24, which has a smaller range than 10.1.0.0/16.
```

The two rules do not specify VPN instances, and specify identical protocol range and source IP address range. According to the auto matching principle in **Table 5-2**, the system compares the destination IP address ranges in the rules. The destination IP address range specified in the permit rule is smaller than that specified in the deny rule, so the permit rule has a higher precision. The system allocates a smaller ID to the permit rule. Therefore, the system arranges the two rules in ACL 3001 in the following order:

```
#
acl number 3001 match-order auto
 rule 5 permit ip destination 10.1.1.0 0.0.0.255
 rule 10 deny ip destination 10.1.0.0 0.0.255.255
#
```

 Copyright © Huawei Technologies Co., Ltd. 

A rule **rule deny ip destination 10.1.1.1 0** is added to ACL 3001 (with a higher priority than the previous two rules because the destination IP address is a host address). The system reassigns IDs to the rules according to the rule priorities. The new order is as follows:

```
#
acl number 3001 match-order auto
 rule 5 deny ip destination 10.1.1.1 0
 rule 10 permit ip destination 10.1.1.0 0.0.0.255
 rule 15 deny ip destination 10.1.0.0 0.0.255.255
#
```

Compared with the config mode, auto mode is more complex; however, it offers advantages in some scenarios. For example, in the initial network deployment stage, the administrator has configured an ACL in auto mode to discard all IP packets in untrusted network segments to ensure network security. When more services are deployed on the network, some IP packets on these network segments need to be allowed. The administrator needs to add new rules to the ACL, but does not need to rearrange the rules to avoid incorrect packet discarding.

## 5.2.5 Matching Conditions

The device supports various ACL matching conditions. This section describes the commonly used conditions.

### Time Range

Format: **time-range** *time-name*

All ACLs support packet filtering based on time ranges. For details about time ranges, see **5.2.6 Time Range**.

### Protocol Type Carried by IP

Format: *protocol-number* | **icmp** | **tcp** | **udp** | **gre** | **igmp** | **ip** | **ipinip** | **ospf**

An advanced ACL can filter packets based on protocol types, such as ICMP (protocol number 1), TCP (protocol number 6), UDP (protocol number 17), GRE (protocol number 47), IGMP (protocol number 2), IP (any IP layer protocol), IPinIP (protocol number 4), and OSPF (protocol number 89). The protocol number ranges from 1 to 255.

For example, to forbid user access on an interface connected to a large number of attackers, specify the protocol type as IP to discard all IP traffic on the interface. The configuration is as follows:

```
rule deny ip //Reject IP packets.
```

After transparent firewall function is enabled on a device, the transparent firewall discards all packets entering the interzone by default, including service and protocol packets. If you require the packets of a dynamic routing protocol, such as OSPF, to pass through the transparent firewall, specify the protocol type as OSPF.

```
rule permit ospf  //Permit OSPF packets.
```

### Source/Destination IP Addresses and Wildcard Masks

Format of source IP address and wildcard mask: **source** { *source-address source-wildcard* | **any** }

 Copyright © Huawei Technologies Co., Ltd. 

Format of destination IP address and wildcard mask: **destination** { *destination-address destination-wildcard* | **any** }

A basic ACL can filter packets based on source IP addresses; an advanced ACL can filter packets based on both source and destination IP addresses.

When the source and destination IP addresses are specified as matching conditions, the wildcard masks must be specified for them to determine address ranges.

The IP address wildcard mask format is the same as the inverse subnet mask format (32-bit numeric string). The wildcard mask specifies the digits in the IP address to be checked. Among the bits in a mask, the value 0 indicates "check" and the value 1 indicates "not check." An IP address subnet mask must have continuous 0s and 1s, whereas a wildcard mask can have discontinuous 0s and 1s.

The wildcard mask can be 255.255.255.255 or 0 (equivalent to 0.0.0.0). The value 255.255.255.255 indicates any IP address, which is equivalent to the **any** keyword. The value 0 indicates that the source/destination address is a host address.

For example, configure a rule with an IP address wildcard mask specified to permit all IP packets from network segment 192.168.1.0/24:

```
rule 5 permit ip source 192.168.1.0 0.0.0.255
```

In this rule, the wildcard mask is 0.0.0.255, indicating that only the bits in the binary bytes in the first three groups in the IP address are checked. Therefore, if the first 24 bits in the source IP address are the same as the first 24 bits in the specified IP address (192.168.1), it indicates that the packets are sent from source IP address segment 192.168.1.0/24, and are permitted. **Table 5-3** illustrates how the address range is calculated.

**Table 5-3** Wildcard mask example

| Item | Decimal | Binary |
| --- | --- | --- |
| Specified IP address | 192.168.1.0 | 11000000.10101000.00000001.00000000 |
| Wildcard mask | 0.0.0.255 | 00000000.00000000.00000000.**11111111** |
| Determined address range | 192.168.1.*<br>* indicates an integer between 0 and 255. | 11000000.10101000.00000001.**xxxxxxxx**<br>x can be 0 or 1. |

For more examples of determining an address range by IP address and wildcard mask, see **Table 5-4**.

**Table 5-4** Determining address ranges by IP addresses and wildcard masks

| IP Address | IP Address Wildcard Mask | Determined Address Range |
| --- | --- | --- |
| 0.0.0.0 | 255.255.255.255 | Any IP address |

 Copyright © Huawei Technologies Co., Ltd. 

| IP Address | IP Address Wildcard Mask | Determined Address Range |
| --- | --- | --- |
| 172.18.0.0 | 0.0.255.255 | IP addresses on network segment 172.18.0.0/16 |
| 172.18.5.2 | 0.0.0.0 | Only host address 172.18.5.2 |
| 172.18.8.0 | 0.0.0.7 | IP addresses on network segment 172.18.8.0/29 |
| 172.18.8.8 | 0.0.0.7 | IP addresses on network segment 172.18.8.8/29 |
| 10.1.2.0 | 0.0.254.255 (discontinuous 1s and 0s in wildcard mask) | IP addresses that are in the range of 10.1.0.0/24 and 10.1.254.0/24 and have an even number in the third byte, for example, 10.1.0.0/24, 10.1.2.0/24, 10.1.4.0/24, and 10.1.6.0/24 |

## Source/Destination MAC Addresses and Wildcard Masks

Format of source MAC address and wildcard mask: **source-mac** *source-mac-address* [ *source-mac-mask* ]

Format of destination MAC address and wildcard mask: **destination-mac** *dest-mac-address* [ *dest-mac-mask* ]

Only the Layer 2 ACL can filter packets based on source and destination MAC addresses.

When the source and destination MAC addresses are specified as matching conditions, the wildcard masks can be specified for them to determine address ranges.

The formats of a MAC address wildcard mask and a MAC address are the same. Both of them are in hexadecimal format. A MAC address wildcard mask consists of six bytes (48 bits) to indicate the bits in a MAC address to be checked. Different from those in an IP address wildcard mask, the value 1 in the MAC address wildcard mask indicates "check" and the value 0 indicates "not check." If the wildcard mask is not specified, the default mask ffff-ffff-ffff is used, indicating that every bit in a MAC address is checked.

Table 5-5 illustrates how a MAC address and a wildcard mask determine an address range.

**Table 5-5** Determining address ranges by MAC addresses and wildcard masks

| MAC Address | MAC Address Wildcard Mask | Determined Address Range |
| --- | --- | --- |
| 00e0-fc01-0101 | 0000-0000-0000 | Any MAC address |

 Copyright © Huawei Technologies Co., Ltd. 

| MAC Address | MAC Address Wildcard Mask | Determined Address Range |
| --- | --- | --- |
| 00e0-fc01-0101 | ffff-ffff-ffff | Only 00e0-fc01-0101 |
| 00e0-fc01-0101 | ffff-ffff-0000 | 00e0-fc01-0000 to 00e0-fc01-ffff |

## VLAN ID and Mask

Format of outer VLAN ID and mask: **vlan-id** *vlan-id* [ *vlan-id-mask* ]

A Layer 2 ACL can filter packets based on outer VLAN IDs.

When the VLAN IDs are configured as matching conditions, the VLAN mask can be specified behind the VLAN IDs to determine a VLAN range.

A VLAN mask is in the hexadecimal format, ranging from 0x0 to 0xFFF. If the VLAN mask is not specified, the default mask 0xFFF is used, indicating that every bit in the VLAN ID is checked.

Table 5-6 illustrates how a VLAN ID and a mask determine a VLAN range.

**Table 5-6** Determining VLAN ranges by VLAN IDs and masks

| VLAN ID | VLAN Mask | Determined VLAN Range |
| --- | --- | --- |
| 10 | 0x000 | Any VLAN |
| 10 | 0xFFF | Only VLAN 10 |
| 10 | 0xFF0 | VLAN 1 to VLAN 15 |

## TCP/UDP Port Number

Format of source port number: **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }

Format of destination port number: **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }

When the protocol type of an advanced ACL is specified as TCP or UDP, the device can filter packets based on TCP or UDP source/destination port numbers.

The operators of specifying TCP/UDP port numbers are as follows:

- **eq** *port*: equivalent to the source/destination port number.
- **gt** *port*: greater than the destination/source port number.
- **lt** *port*: less than the source/destination port number.
- **range** *port-start port-end*: source/destination port number range. *port-start* indicates the start port number, and *port-end* indicates the end port number.

The TCP/UDP port numbers can be represented by numeric or character strings (alias). For example, **rule deny tcp destination-port eq 80** can be represented by

 Copyright © Huawei Technologies Co., Ltd. 

**rule deny tcp destination-port eq www**. **Table 5-7** and **Table 5-8** list the commonly used TCP ports and UDP ports respectively, and provide the corresponding character strings.

**Table 5-7** Commonly used TCP ports and character strings

| Port Number | Character String | Protocol | Description |
| --- | --- | --- | --- |
| 7 | echo | Echo | Echo service. |
| 9 | discard | Discard | Null service used for connectivity test. |
| 13 | daytime | Daytime | Daytime protocol. |
| 19 | CHARgen | Character generator | Character Generator Protocol. |
| 20 | ftp-data | FTP data connections | FTP data port. |
| 21 | ftp | File Transfer Protocol(FTP) | File Transfer Protocol (FTP) port. |
| 23 | telnet | Telnet | Telnet service. |
| 25 | smtp | Simple Mail Transport Protocol (SMTP) | Simple Mail Transfer Protocol (SMTP). |
| 37 | time | Time | Time protocol. |
| 43 | whois | Nickname (WHOIS) | Directory service. |
| 49 | tacacs | TAC Access Control System (TACACS) | Access control system based on TCP/IP authentication (TACACS login host protocol) |
| 53 | domain | Domain Name Service (DNS) | Domain name service. |
| 70 | gopher | Gopher | Information index protocol (document searching and indexing on the Internet) |
| 79 | finger | Finger | Queries online user information on a remote host. |


Copyright © Huawei Technologies Co., Ltd.

| Port Number | Character String | Protocol | Description |
| --- | --- | --- | --- |
| 80 | www | World Wide Web (HTTP) | Protocol used by the WWW service. HTTP is used to browse web pages. |
| 101 | hostname | NIC hostname server | Host name service on the NIC machine. |
| 109 | pop2 | Post Office Protocol v2 | Email protocol version 2. |
| 110 | pop3 | Post Office Protocol v3 | Email protocol version 3. |
| 111 | sunrpc | Sun Remote Procedure Call (RPC) | RPC protocol of SUN. It is used to remotely execute commands and used by the network file system (NFS). |
| 119 | nntp | Network News Transport Protocol (NNTP) | Network News Transfer Protocol for retrieval of newsgroup messages. It carries USENET. |
| 179 | bgp | Border Gateway Protocol (BGP) | Border Gateway Protocol (BGP). |
| 194 | irc | Internet Relay Chat (IRC) | Internet Relay Chat (IRC) protocol. |
| 512 | exec | Exec (rsh) | Authenticates remote process. |
| 513 | login | Login (rlogin) | Remote login. |
| 514 | cmd | Remote commands | Used to execute non-interactive commands on a remote system (rshell, rcp). |
| 515 | lpd | Printer service | Line Printer Daemon. It is a print service. |
| 517 | talk | Talk | Remotely talks with server and client. |


Copyright © Huawei Technologies Co., Ltd.

| Port Number | Character String | Protocol | Description |
| --- | --- | --- | --- |
| 540 | uucp | Unix-to-Unix Copy Program | Unix-to-Unix copy protocol. |
| 543 | klogin | Kerberos login | Kerberos login protocol version 5. |
| 544 | kshell | Kerberos shell | Kerberos Remote shell protocol version 5. |

**Table 5-8** Commonly used UDP ports and character strings

| Port Number | Character String | Protocol | Description |
| --- | --- | --- | --- |
| 7 | echo | Echo | Echo service. |
| 9 | discard | Discard | Null service used for connectivity test. |
| 37 | time | Time | Time protocol. |
| 42 | nameserver | Host Name Server | Host name service. |
| 53 | dns | Domain Name Service (DNS) | Domain name service. |
| 65 | tacacs-ds | TACACS-Database Service | TACACS database service. |
| 67 | bootps | Bootstrap Protocol Server | Bootstrap Protocol (BOOTP) Server, also used by Dynamic Host Configuration Protocol (DHCP). |
| 68 | bootpc | Bootstrap Protocol Client | Bootstrap Protocol (BOOTP) Client, also used by Dynamic Host Configuration Protocol (DHCP). |
| 69 | tftp | Trivial File Transfer Protocol (TFTP) | Trivial File Transfer Protocol (TFTP). |

 Copyright © Huawei Technologies Co., Ltd. 

| Port Number | Character String | Protocol | Description |
| --- | --- | --- | --- |
| 90 | dnsix | DNSIX Security Attribute Token Map | DoD Network Security for Information Exchange (DNSIX) Security Attribute Token Map. |
| 111 | sunrpc | SUN Remote Procedure Call (SUN RPC) | RPC protocol of SUN. It is used to remotely execute commands and used by the network file system (NFS). |
| 123 | ntp | Network Time Protocol (NTP) | Network Time Protocol (NTP), which may be utilized by worm virus. |
| 137 | netbios-ns | NETBIOS Name Service | NETBIOS name service. |
| 138 | netbios-dgm | NETBIOS Datagram Service | NETBIOS datagram service. |
| 139 | netbios-ssn | NETBIOS Session Service | NETBIOS session service. |
| 161 | snmp | SNMP | Simple Network Management Protocol (SNMP). |
| 162 | snmptrap | SNMPTRAP | SNMP trap. |
| 177 | xdmcp | X Display Manager Control Protocol (XDMCP) | X Display Manager Control Protocol (XDMCP). |
| 434 | mobilip-ag | MobileIP-Agent | Mobile IP agent. |
| 435 | mobilip-mn | MobileIP-MN | Mobile IP management. |
| 512 | biff | Mail notify | Notifies user of received emails. |
| 513 | who | Who | Login user list. |
| 514 | syslog | Syslog | UNIX system log service. |
| 517 | talk | Talk | Remotely talks with server and client. |


Copyright © Huawei Technologies Co., Ltd.

| Port Number | Character String | Protocol | Description |
| --- | --- | --- | --- |
| 520 | rip | Routing Information Protocol | RIP routing protocol. |

## TCP Flag

Format: **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** }*

When the TCP protocol is specified in an advanced ACL, the device filters packets based on the TCP flag.

A TCP packet header contains six flag bits:

- URG(100000): indicates that the Urgent pointer field is significant.
- ACK(010000): indicates that the Acknowledgment field is significant.
- PSH(001000): push function. Asks to push the buffered data to the receiving application.
- RST(000100): resets the connection.
- SYN(000010): synchronizes sequence numbers to initiate a connection.
- FIN(000001): no more data from sender.

The **established** field in TCP flags indicates that the flag bit is ACK(010000) or RST(000100).

The ACL rule with the **tcp-flag** keyword specified can implement unidirectional access control. For example, it is required that users on network segment 192.168.1.0/24 can access network segment 192.168.2.0/24, but users on network segment 192.168.2.0/24 cannot access network segment 192.168.1.0/24. To meet this requirement, you can apply an ACL rule to the inbound direction of the interface connecting to network segment 192.168.2.0/24.

From TCP connection setup to teardown only the packets used for TCP connection establishment can have the ACK value of 1 and RST value of 1. According to this characteristic, configure the following ACL rules to permit the packets used for establishing TCP connections and deny other TCP packets on the network segment 192.168.2.0/24. In this way, you can limit the TCP connection requests initiated from this network segment.

- Rule 1: Configure an ACL rule with the **ack** and **rst** keywords specified.

  ```
  rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack  //Permit the TCP packets with the ACK value of 1.
  rule 10 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst  //Permit the TCP packets with the RST value of 1.
  rule 15 deny tcp source 192.168.2.0 0.0.0.255  //Reject other TCP packets.
  ```

- Rule 2: Configure an ACL rule with the **established** keyword specified.

  ```
  rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag established  //established indicates that ACK is 1 or RST is 1. The packets exchanged during TCP connection established are permitted.
  rule deny tcp source 192.168.2.0 0.0.0.255     //Reject other TCP packets.
  ```

## IP Fragmentation

Format: **none-first-fragment**

 Copyright © Huawei Technologies Co., Ltd. 

A basic ACL and an advanced ACL can filter packets based on IP fragmentation information.

The fragments of an IP packet include the initial fragment and non-initial fragments. Only the initial fragment contains Layer 4 information, such as TCP and UDP port numbers. A network device checks whether a received fragment is the last fragment. If the fragment is not the last, the device allocates memory space for it, and reassembles the fragments after the last fragment is received. However, an exploit exists whereby an attacker may send fragments to a device without sending the last fragment. Because the device cannot release memory until the last fragment is received and all fragments are reassembled, if a large enough number of fragments are sent in a short period, the device cannot process other services due to insufficient memory resources. To mitigate such an attack, the device starts a reassembling timer. If reassembly cannot be finished before the timer expires, the device returns an ICMP Error packet to the sender; if reassembly cannot be finished after the timer expires, the device discards the fragments stored in memory.

To prevent fragment packet attacks, you can specify the **none-first-fragment** keyword in an ACL rule to block non-initial fragments.

**Table 5-9** describes how the ACLs process non-fragment packets, initial fragments, and non-initial fragments.

**Table 5-9** IP packet processing methods

| Matching Conditions | Non-fragment Packets | Initial Fragments | Non-initial Fragments |
| --- | --- | --- | --- |
| Layer 3 information (such as source/ destination IP addresses) | When packets match Layer 3 information, the matching result (permit or deny) is returned; otherwise, the next rule is processed. | When packets match Layer 3 information, the matching result (permit or deny) is returned; otherwise, the next rule is processed. | When packets match Layer 3 information, the matching result (permit or deny) is returned; otherwise, the next rule is processed. |
| Layer 3 information and Layer 4 information (such as TCP and UDP port numbers) | When packets match both Layer 3 and Layer 4 information, the matching result (permit or deny) is returned; otherwise, the next rule is processed. | When packets match both Layer 3 and Layer 4 information, the matching result (permit or deny) is returned; otherwise, the next rule is processed. | The packets do not match the rule, so the next rule is processed. |

 Copyright © Huawei Technologies Co., Ltd. 

| Matching Conditions | Non-fragment Packets | Initial Fragments | Non-initial Fragments |
| --- | --- | --- | --- |
| Layer 3 information and **none-first-fragment** | The packets do not match the rule, so the next rule is processed. | The packets do not match the rule, so the next rule is processed. | When packets match Layer 3 information, the matching result (permit or deny) is returned; otherwise, the next rule is processed. |

For example, ACL 3012 contains the following rules:

```
#
acl number 3012
 rule 5 deny tcp destination 192.168.2.2 0 none-first-fragment
 rule 10 permit tcp destination 192.168.2.2 0 destination-port eq www
 rule 15 deny ip
#
```

- This packet is a non-fragment packet or initial fragment: If the destination port number is 80 (WWW), this packet matches rule 10 and is permitted; otherwise, the packet matches rule 15 and is discarded.
- The packet is a non-initial fragment: The packet matches rule 5 and is discarded.

## 5.2.6 Time Range

### Background

An ACL contains various matching conditions to filter most packets. However, networks continue to evolve and requirements change. For example, an enterprise allows employees to access only the specified websites during work hours, and to access other websites in off-hours and weekends. Here is another example. The P2P and downloading services affect other data services during the peak hours of 20:00-22:00; therefore, the network administrator is required to lower the bandwidth for the P2P and downloading services in this period.

Time-based ACL can meet the preceding requirements. The network administrators can create one or more time ranges according to users' network access behaviors and network congestion condition, and associate the time ranges with ACL rules. In this way, administrators can configure different policies in different time ranges to optimize networks.

### Time Range Mode

You can associate a time range with ACL rules in either of the following ways:

- Mode 1 - Periodic time range: defines a time range based on weeks. The associated ACL rules take effect at an interval of one week. For example, if the time range of ACL rules is 8:00-12:00 on Monday, the ACL rules take effect at 8:00-12:00 on every Monday.

 Copyright © Huawei Technologies Co., Ltd. 

Format: **time-range** *time-name start-time* **to** *end-time* { *days* } &<1-7>

- *time-name*: indicates the name of a time range. It is a string starting with a letter.
- *start-time* **to** *end-time*: indicates the start and end time of the time range. The format is [hour:minute] to [hour:minute].
- *days*: includes the following values:
  - One of **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, and **Sun** or a combination of them. The value can also be numeric. For example, 0 indicates Sunday, 1 indicates Monday..., and 6 indicates Saturday.
  - **working-day**: from Monday to Friday.
  - **daily**: from Monday to Sunday.
  - **off-day**: Saturday and Sunday.

- Mode 2 - Absolute time range: defines a time range from YYYY/MM/DD hh:mm to YYYY/MM/DD hh:mm. The associated ACL rules take effect only in this period.

  Format: **time-range** *time-name* **from** *time1 date1* [ **to** *time2 date2* ]

  - *time-name*: indicates the name of a time range. It is a string starting with a letter.
  - *time1*|*time2*: The format is [hour:minute].
  - *date1*|*date2*: The format is [YYYY/MM/DD], indicating year/month/date.

You can specify multiple time ranges in the same *time-name* parameter. The device obtains the intersection of the configured periodic or absolute time ranges.

For example, ACL 2001 is associated with time range **test**, which contains three sub-ranges:

```
#
time-range test 8:00 to 18:00 working-day
time-range test 14:00 to 18:00 off-day
time-range test from 00:00 2014/01/01 to 23:59 2014/12/31
#
acl number 2001
 rule 5 permit time-range test
```

- Sub-range 1: 8:00-18:00 from Monday to Friday (periodic time range)
- Sub-range 2: 14:00-18:00 on Saturday and Sunday (periodic time range)
- Sub-range 3: from 2014-1-1 00:00 to 2014-12-31 23:59 (absolute time range)

The time range **test** is: 8:00-18:00 on Monday to Friday and 14:00-18:00 every Saturday and Sunday in 2014.

# 5.2.7 Default ACL Actions and Mechanisms of Different Service Modules

## Applying ACL to Service Modules

After an ACL is configured, it must be applied to a service module so that the ACL rules can be delivered and take effect.

 Copyright © Huawei Technologies Co., Ltd. 

Usually, an ACL is applied to a traffic policy or simplified traffic policy so that the device can deliver ACL rules globally, or on an interface to filter packets to be forwarded. In addition, an ACL can be applied to the service modules such as Telnet, FTP, and routing.

Table 5-10 describes how the service modules process ACLs.

**Table 5-10** Applying ACLs to service modules

| Service Category | Usage Scenario | Service Modules |
| --- | --- | --- |
| Filtering packets to be forwarded | The device filters received packets globally, or on an interface, and then discards, modifies priorities of, or redirects the filtered packets.<br>For example, you can use ACL to reduce the service level for the bandwidth-consuming services, such as P2P downloading and online video. When network congestion occurs, these packets are discarded first. | Traffic policy, simplified traffic policy |
| Filtering packets to be sent to the CPU | If too many protocol packets are sent to the CPU, the CPU usage increases and CPU performance degrades. The device restricts the packets to be sent to the CPU.<br>For example, when a user sends a large number of ARP attack packets to the device, the CPU is busy and service is interrupted. You can apply an ACL to the local attack defense service, and add the user to the blacklist so that the CPU discards the packets from this user. | Blacklist |

 Copyright © Huawei Technologies Co., Ltd. 

| Service Category | Usage Scenario | Service Modules |
| --- | --- | --- |
| Login control | The device controls access permission of users. Only authorized users can log in to the device, and other users cannot log in without permission. This ensures network security.<br>For example, only the administrator is allowed to log in to the device. You can apply an ACL to the Telnet service and specify the hosts that can log in to the device or the hosts that cannot log in. | Telnet, STelnet, FTP, SFTP, HTTP, SNMP |
| Route filtering | ACLs can be applied to various dynamic routing protocols to filter advertised and received routes and multicast groups.<br>For example, you can apply an ACL to a routing policy to prevent the device from sending routes of a network segment to the neighboring router. | BGP, IS-IS, OSPF, OSPFv3, RIP, RIPng, multicast protocol |

## Default ACL Actions and Mechanisms

When an ACL is applied to service modules, the modules take different actions on the packets matching or not matching ACL rules.

For example, the default action of a traffic policy is permit and an ACL containing rules is applied to the traffic policy. If a packet does not match any ACL rules, the packet is permitted. The default action of the Telnet module is deny and an ACL containing rules is applied to the Telnet module. If a packet does not match any ACL rules, the packet is rejected.

The blacklist module processes ACL in a different way. After an ACL is applied to a blacklist, the packets matching any ACL rule are discarded no matter whether they match the permit or deny rule.

**Table 5-11** provides the default ACL actions and mechanisms taken by each service module.


Copyright © Huawei Technologies Co., Ltd.

**Table 5-11** Default ACL actions and mechanisms of different service modules

| Service Module | Default ACL Action | ACL Processing Mechanism | | | | |
|---|---|---|---|---|---|---|
| | | Packets Match the permit Rule | Packets Match the deny Rule | Packets Do Not Match Any Rule in an ACL | An ACL Does Not Contain Rules | ACL Is Not Created |
| Telnet | deny | permit (allowed to log in) | deny (not allowed to log in) | deny (not allowed to log in) | permit (allowed to log in) | permit (allowed to log in) |
| STelnet | deny | permit (allowed to log in) | deny (not allowed to log in) | deny (not allowed to log in) | permit (allowed to log in) | permit (allowed to log in) |
| HTTP | deny | permit (allowed to log in) | deny (not allowed to log in) | deny (not allowed to log in) | permit (allowed to log in) | permit (allowed to log in) |
| SNMP | deny | permit (allowed to log in) | deny (not allowed to log in) | deny (not allowed to log in) | permit (allowed to log in) | permit (allowed to log in) |
| FTP | deny | permit (allowed to log in) | deny (not allowed to log in) | deny (not allowed to log in) | permit (allowed to log in) | permit (allowed to log in) |
| TFTP | deny | permit (allowed to log in) | deny (not allowed to log in) | deny (not allowed to log in) | permit (allowed to log in) | permit (allowed to log in) |
| SFTP | deny | permit (allowed to log in) | deny (not allowed to log in) | deny (not allowed to log in) | permit (allowed to log in) | permit (allowed to log in) |

 Copyright © Huawei Technologies Co., Ltd. 

| Service Module | Default ACL Action | ACL Processing Mechanism | | | | |
|---|---|---|---|---|---|---|
| | | Packets Match the permit Rule | Packets Match the deny Rule | Packets Do Not Match Any Rule in an ACL | An ACL Does Not Contain Rules | ACL Is Not Created |
| Traffic policy | permit | • When the traffic behavior is permit, the packets are forwarded.<br>• When the traffic behavior is deny, the packets are discarded.<br>• When the traffic behavior is neither permit nor deny, the packets are forwarded (action in traffic policy). | deny (discarded)<br>**NOTE**<br>The device takes the action defined in the traffic behavior only when the traffic behavior is traffic statistics collection or mirroring. | permit (traffic policy does not take effect, and packets are forwarded without the restriction of traffic policy) | permit (traffic policy does not take effect, and packets are forwarded without the restriction of traffic policy) | permit (traffic policy does not take effect, and packets are forwarded without the restriction of traffic policy) |


Copyright © Huawei Technologies Co., Ltd.

| Service Module | Default ACL Action | ACL Processing Mechanism | | | | |
|---|---|---|---|---|---|---|
| | | Packets Match the permit Rule | Packets Match the deny Rule | Packets Do Not Match Any Rule in an ACL | An ACL Does Not Contain Rules | ACL Is Not Created |
| Simplified traffic policy | permit | permit (the device takes the action defined in the simplified traffic policy) | • When the action in the simplified traffic policy is traffic-filter or traffic-secure: deny<br>• When the action in the simplified traffic policy is neither traffic-filte | permit (simplified traffic policy does not take effect, and packets are forwarded without the restriction of simplified traffic policy) | permit (simplified traffic policy does not take effect, and packets are forwarded without the restriction of simplified traffic policy) | permit (simplified traffic policy does not take effect, and packets are forwarded without the restriction of simplified traffic policy) |


Copyright © Huawei Technologies Co., Ltd.

| Service Module | Default ACL Action | ACL Processing Mechanism | | | | |
|---|---|---|---|---|---|---|
| | | Packets Match the permit Rule | Packets Match the deny Rule | Packets Do Not Match Any Rule in an ACL | An ACL Does Not Contain Rules | ACL Is Not Created |
| | | | r nor traffic-secure: permit | | | |
| Local attack defense policy (blacklist) | permit | deny (discarded) | deny (discarded) | permit (blacklist does not take effect, and packets are forwarded) | permit (blacklist does not take effect, and packets are forwarded) | permit (blacklist does not take effect, and packets are forwarded) |
| NAT Server | permit | permit (NAT) | deny (no NAT) | deny (no NAT) | permit (NAT) | permit (NAT) |

 Copyright © Huawei Technologies Co., Ltd. 

| Service Module | | Default ACL Action | ACL Processing Mechanism | | | | |
|---|---|---|---|---|---|---|---|
| | | | Packets Match the permit Rule | Packets Match the deny Rule | Packets Do Not Match Any Rule in an ACL | An ACL Does Not Contain Rules | ACL Is Not Created |
| Routing | Route Policy | deny | • When the matching mode is permit: permit (routing policy is enforced)<br>• When the matching mode is deny: deny (routing policy is not enforced) | deny (routing policy does not take effect) | deny (routing policy does not take effect) | permit (routing policy takes effect on all routes) | deny (routing policy does not take effect) |
| | Filter Policy | deny | permit (route advertisement or reception is allowed) | deny (route advertisement or reception is not allowed) | deny (route advertisement or reception is not allowed) | deny (route advertisement or reception is not allowed) | permit (route advertisement or reception is allowed) |


Copyright © Huawei Technologies Co., Ltd.

| Service Module | | Default ACL Action | ACL Processing Mechanism | | | | |
|---|---|---|---|---|---|---|---|
| | | | Packets Match the permit Rule | Packets Match the deny Rule | Packets Do Not Match Any Rule in an ACL | An ACL Does Not Contain Rules | ACL Is Not Created |
| Multicast | igmp-snooping ssm-policy | deny | permit (added to SSM group address range) | deny (not added to SSM group address range) | deny (not added to SSM group address range) | deny (not added to SSM group address range, and no group is in the SSM group address range) | deny (not added to SSM group address range, and only the temporary group addresses 232.0.0.0-232.255.255.255 are in the SSM group address range) |
| | igmp-snooping group-policy | permit | permit (added to multicast group) | deny (not added to multicast group) | permit (added to multicast group) | permit (added to multicast group) | permit (added to multicast group) |

## 5.2.8 ACL Configuration Guidelines

When configuring ACL rules, follow these guidelines:

1. The rules in an ACL may overlap. If packets match the rules with loose conditions, the later ACL rules are not processed. In this case, packets cannot match the rules with strict conditions. Therefore, the rules with strict conditions must be arranged in front lines and those with loose conditions must be arranged towards the end.
2. The ACL configuration guidelines vary according to the default ACL actions taken by the service modules (for details, see **5.2.7 Default ACL Actions and Mechanisms of Different Service Modules**). For example, if a service module


Copyright © Huawei Technologies Co., Ltd.

with the default action of permit must deny the packets from some IP addresses, deny rules only for these IP addresses need to be configured; a permit rule for any IP address is not required. The converse is true for a service module whose default action is deny. **Table 5-12** describes the ACL configuration guidelines.

NOTE

The following rules are for reference. Adhere to the command line syntax when configuring ACL rules.

- **rule permit xxx**/**rule permit xxxx**: allows the specified packets to pass. xxx/xxxx indicates packet attributes, such as source IP address, source MAC address, and time range. The range xxxx involves the range xxx. For example, if xxx is an IP address, xxxx is the network segment where the IP address resides or **any** (any IP address); if xxx is a time range on Saturday, xxxx is all day long on weekends or from Monday to Sunday.
- **rule deny xxx**/**rule deny xxxx**: blocks the specified packets.
- **rule permit**: allows all packets to pass.
- **rule deny**: blocks all packets.

**Table 5-12** ACL configuration guidelines

| Default ACL Action | Permit All Packets | Deny All Packets | Permit a Few Packets and Deny Most Packets | Deny a Few Packets and Permit Most Packets |
|---|---|---|---|---|
| **permit** | No ACL is required. | Configure **rule deny**. | Configure **rule permit xxx** first, and then **rule deny xxxx** or **rule deny**.<br>**NOTE**<br>This guideline applies to packet filtering. When an ACL is applied to traffic policing or traffic statistics collection in a traffic policy, configure **rule permit xxx** if you only need to count rate or collect statistics on the specified packets. | Only **rule deny xxx** is required, and **rule permit xxxx** or **rule permit** is not required.<br>**NOTE**<br>If **rule permit** is configured and ACL is applied to a traffic policy in which the behavior is **deny**, all packets are rejected and all services are interrupted. |

 Copyright © Huawei Technologies Co., Ltd. 

| Default ACL Action | Permit All Packets | Deny All Packets | Permit a Few Packets and Deny Most Packets | Deny a Few Packets and Permit Most Packets |
| --- | --- | --- | --- | --- |
| **deny** | • Routing and multicast module: Configure **rule permit**.<br>• Other modules: ACL is not required. | • Routing and multicast modules: ACL is not required.<br>• Other modules: Configure **rule deny**. | Only **rule permit xxx** is required, and **rule deny xxxx** or **rule deny** is not required. | Configure **rule deny xxx** first, and then **rule permit xxxx** or **rule permit**. |

Example:

- Example 1: Apply an ACL to a traffic policy to filter packets from network segment 192.168.1.0/24. Reject the packets from hosts 192.168.1.2 and 192.168.1.3, and allow the packets from other hosts on network segment 192.168.1.0/24 to pass.

  The default ACL action of the traffic policy module is **permit**, and a few packets are denied and most packets are permitted. Therefore, you only need to configure **rule deny xxx**.

  ```
  #
  acl number 2000
   rule 5 deny source 192.168.1.2 0
   rule 10 deny source 192.168.1.3 0
  #
  ```

- Example 2: Apply an ACL to a traffic policy to filter packets from network segment 192.168.1.0/24. Allow the packets from hosts 192.168.1.2 and 192.168.1.3 to pass, and reject the packets from other hosts on network segment 192.168.1.0/24.

  The default ACL action of the traffic policy module is **permit**, and a few packets are permitted and most packets are denied. Therefore, you need to configure **rule permit xxx** first, and then **rule deny xxxx**.

  ```
  #
  acl number 2000
   rule 5 permit source 192.168.1.2 0
   rule 10 permit source 192.168.1.3 0
   rule 15 deny source 192.168.1.0 0.0.0.255
  #
  ```

- Example 3: Apply an ACL to Telnet, to allow only the administrator's host (172.16.105.2) to Telnet to the device and reject other users.

  The default ACL action of the Telnet module is **deny**, and a few packets are permitted and most packets are denied. Therefore, you only need to configure **rule permit xxx**.

  ```
  #
  acl number 2000
   rule 5 permit source 172.16.105.2 0
  #
  ```

 Copyright © Huawei Technologies Co., Ltd. 

- Example 4: Apply an ACL to Telnet, to forbid two hosts (172.16.105.3 and 172.16.105.4) to Telnet to the device and allow other user hosts to Telnet to the device.

  The default ACL action of the Telnet module is **deny**, and a few packets are denied and most packets are permitted. Therefore, you need to configure **rule deny xxx** first, and then **rule permit**.

  ```
  #
  acl number 2000
   rule 5 deny source 172.16.105.3 0
   rule 10 deny source 172.16.105.4 0
   rule 15 permit
  #
  ```

- Example 5: Apply an ACL to FTP to prevent users from accessing the FTP server from 00:00-08:00 every Saturday.

  The default ACL action of the FTP module is **deny**, and a few packets are denied and most packets are permitted. Therefore, you need to configure **rule deny xxx** first, and then **rule permit xxxx**.

  ```
  #
  time-range t1 00:00 to 08:00 Sat
  time-range t2 00:00 to 23:59 daily
  #
  acl number 2000
   rule 5 deny time-range t1
   rule 10 permit time-range t2
  #
  ```

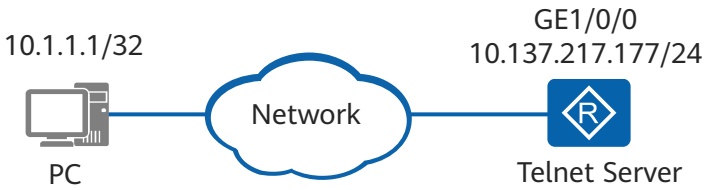
# 5.3 Application Scenarios for ACLs

## 5.3.1 Using an ACL to Control Telnet Login Rights

To allow only specified Telnet clients to access a Telnet server, you can apply an ACL to the Telnet module.

In **Figure 5-4**, to manage the remote Telnet server conveniently, the administrator configures AAA authentication on the Telnet server. Only the Telnet users passing the AAA authentication can log in to the server. In addition, an ACL-based login control policy is configured on the server so that only the administrator's PC can log in to the server.

**Figure 5-4** Using an ACL to control Telnet login rights



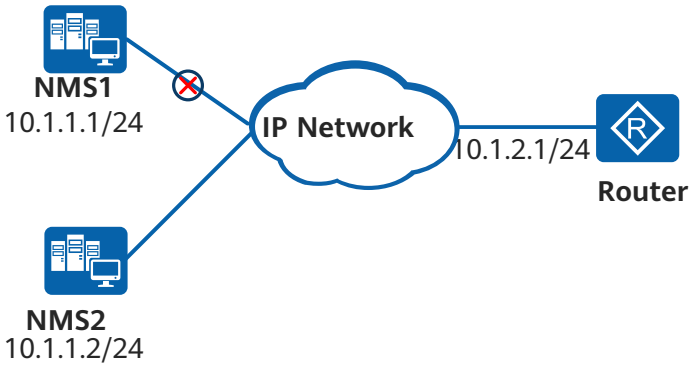

## 5.3.2 Applying an ACL to SNMP to Filter NMSs


Copyright © Huawei Technologies Co., Ltd.

To control which NMSs can access a device, you can apply an ACL to the SNMP module.

In **Figure 5-5**, to manage the remote Router conveniently, the administrator configures the SNMP agent service on the Router so that the agent can report the Router's status to the NMS in a timely manner and the NMS can remotely control the Router. In addition, an ACL-based NMS access right control is configured to allow only the trusted NMS (NMS2) to manage the Router.

**Figure 5-5** Applying an ACL to SNMP to filter NMSs



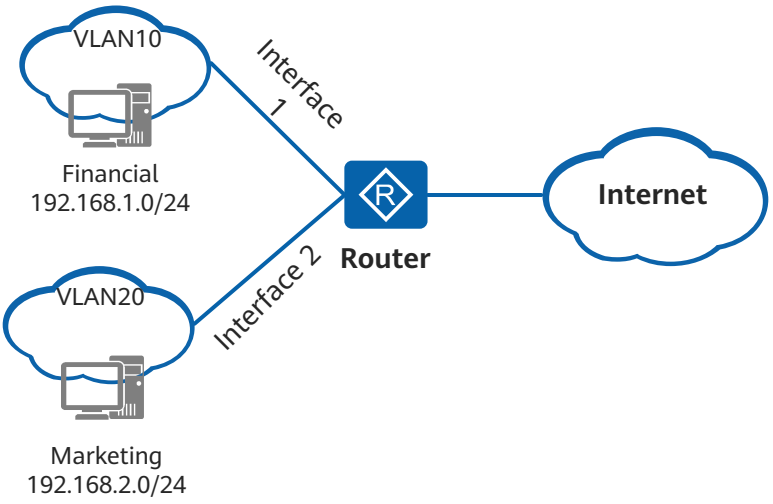

## 5.3.3 Using an ACL to Restrict Mutual Access Between Network Segments

Unrestricted mutual access between different network segments brings security risks. To restrict users' access to network segments on which they do not reside, you can apply an ACL to a traffic policy or simplified traffic policy.

In **Figure 5-6**, the financial department and the marketing department reside on separate network segments. Information leak may occur if the two departments have unrestricted access to each other. Therefore, to restrict mutual access between the two departments, an ACL-based traffic policy or simplified traffic policy is applied in the inbound direction of the interfaces (Interface 1 and Interface 2).

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 5-6** Using an ACL to restrict mutual access between network segments

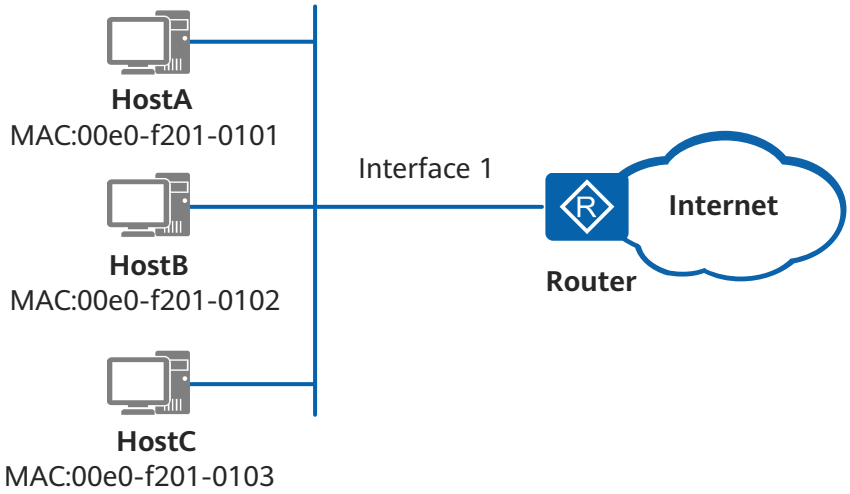



## 5.3.4 Using an ACL to Prevent Certain Users from Accessing the Internet in the Specified Time Range

To prevent certain users from accessing the Internet in a specified time range, you can apply an ACL to a traffic policy or simplified traffic policy.

In **Figure 5-7**, the enterprise intranet connects to the Internet through a router. Some employees access non-work-related websites in work hours, lowering their work efficiency. Therefore, to prevent these employees from accessing the Internet in work hours and allow access in off-hours, a time-based ACL is configured and an ACL-based traffic policy or simplified traffic policy is applied to the inbound direction of Interface 1, which connects to these employees.

**Figure 5-7** Using an ACL to prevent certain users from accessing the Internet in the specified time range





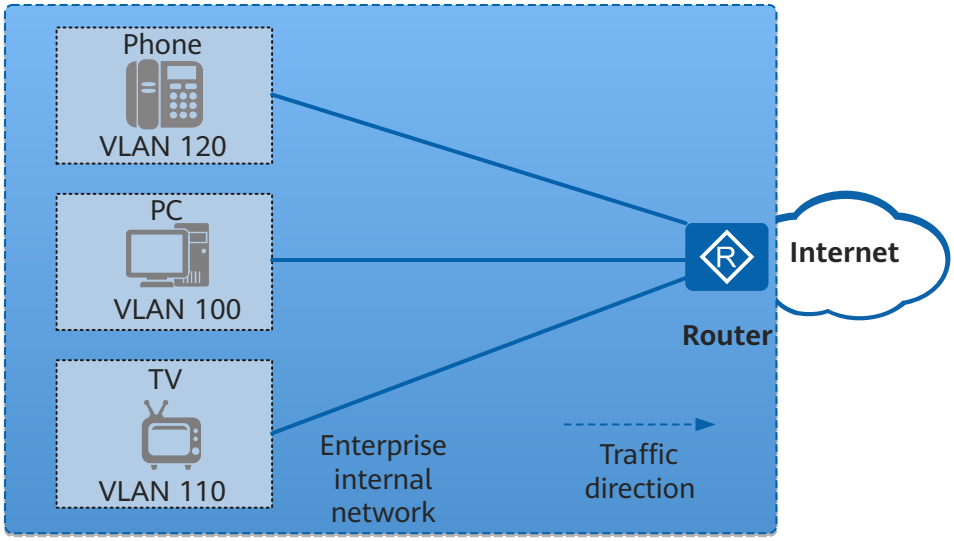
Copyright © Huawei Technologies Co., Ltd.

## 5.3.5 Using an ACL in QoS to Implement Traffic Policing

To monitor the rate of different traffic entering the network and penalize excess traffic, you can apply an ACL to a traffic policy or simplified traffic policy. In this way, you can restrict the rate of traffic entering the network to guarantee network resources.

In **Figure 5-8**, VLAN 100, VLAN 110, and VLAN 120 of an enterprise network provide the data, video, and voice services, respectively. ACL-based traffic policing is configured to ensure the service quality of data is higher than that of video, and that of video is higher than that of voice. ACL-based traffic policing classifies different service flows of the enterprise based on VLAN IDs and limits the rate of packets that match ACL rules. In this way, the traffic rates of different services can be controlled and bandwidth for the services can be guaranteed.

**Figure 5-8** Using an ACL in QoS to implement traffic policing




## 5.3.6 Using an ACL to Filter OSPF Routes

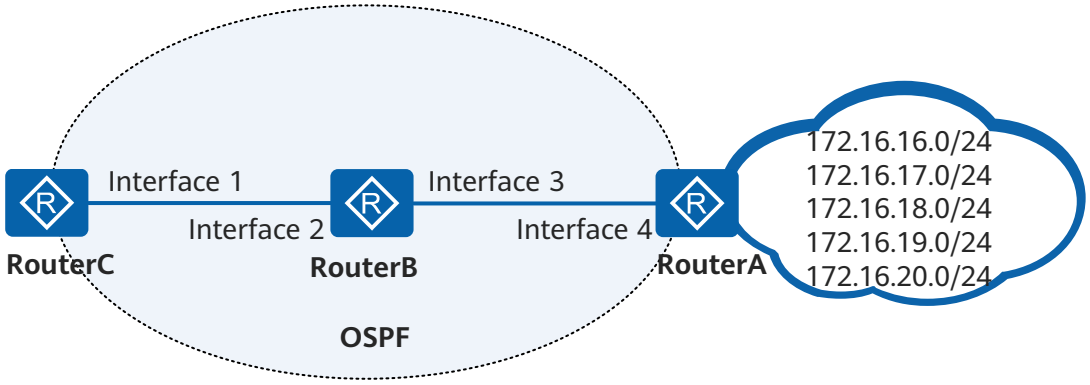
An ACL can be applied to various dynamic routing protocols to filter advertised and received routes.

In **Figure 5-9**, the network runs the Open Shortest Path First (OSPF) protocol. RouterA receives routes from the Internet and advertises the routes to the OSPF network. The OSPF network is allowed to access only three network segments: 172.16.17.0/24, 172.16.18.0/24, and 172.16.19.0/24. The network connected to RouterC is allowed to access only the network segment 172.16.18.0/24.

To meet the preceding requirements, an ACL and a routing policy are configured on RouterA. This routing policy permits RouterA to advertise only the routes on network segments 172.16.17.0/24, 172.16.18.0/24, and 172.16.19.0/24 to RouterB, so that the OSPF network can access only these three network segments. An ACL and a routing policy are also configured on RouterC. The routing policy permits RouterC to receive only the route 172.16.18.0/24, so that the network connected to RouterC can access only the network segment 172.16.18.0/24.


Copyright © Huawei Technologies Co., Ltd.

**Figure 5-9** Using an ACL to filter OSPF routes




## 5.3.7 Using ACL in NAT to Filter Traffic

After an ACL is applied to NAT, the NAT device filters the traffic from the external network to the internal network.

A NAT device filters the traffic from external network to internal network. There are three NAT modes:

- Endpoint-independent filtering
- Address-dependent filtering
- Address and port-dependent filtering

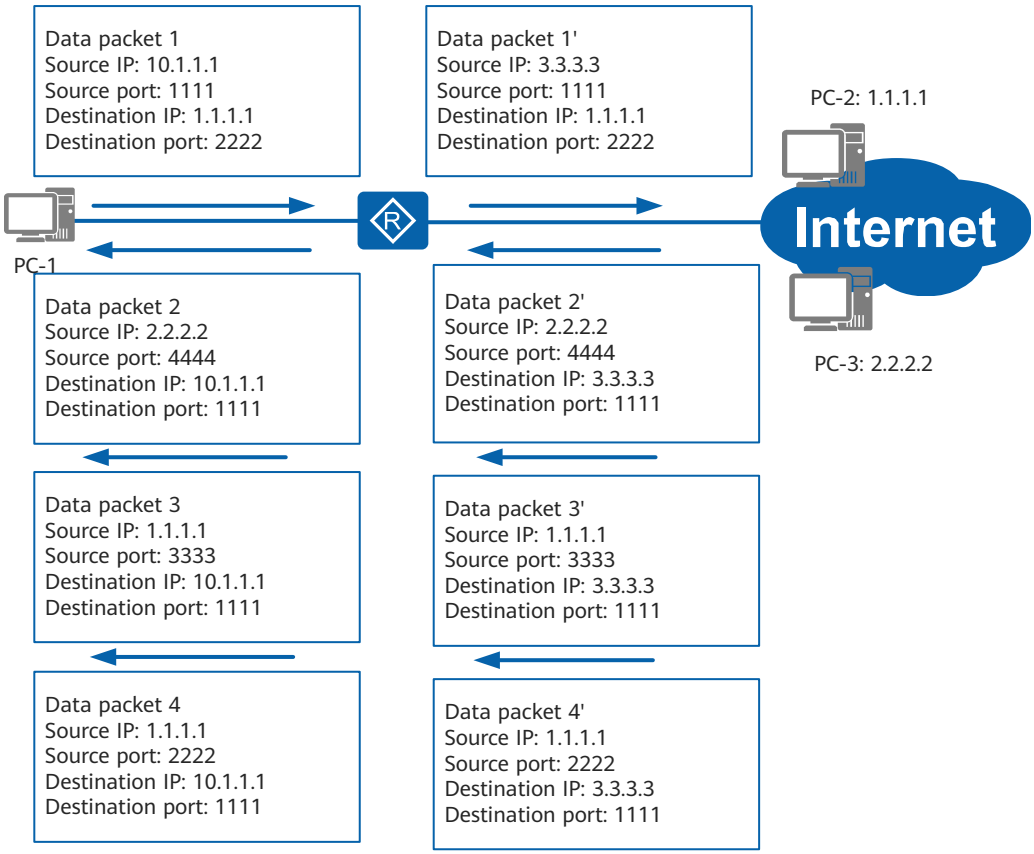
In **Figure 5-10**, PC-1 on the private network communicates with PC-2 and PC-3 on the external network through a NAT device. Datagram 1 is sent from PC-1 to PC-2. The source port number of the datagram is 1111 and the destination port number is 2222. The NAT device translates the source IP address to 10.169.10.1.

After PC-1 sends an access request to a PC on the external network, the PC on the external network transmits traffic to PC-1. The NAT device filters the traffic to PC-1. Datagram 2', datagram 3', and datagram 4' are sent in three scenarios.

- Datagram 2' is sent from PC-3 to PC-1. The destination address of datagram 2' is different from that of datagram 1, and the destination port number is 1111. The datagram can pass the NAT device only when the endpoint-independent filtering mode is used.
- Datagram 3' is sent from PC-2 to PC-1. The destination address of datagram 3' is the same as that of datagram 1, and the destination port number is 1111. The source port number of datagram 3' is 3333, which is different from that of datagram 1. The datagram can pass the NAT device only when the Address-dependent filtering or endpoint-independent filtering mode is used.
- Datagram 4' is sent from PC-2 to PC-1. The destination address of datagram 4' is the same as that of datagram 1, and the destination port number is 1111. The source port number of datagram 4' is 2222, which is the same as that of datagram 1. The datagram can pass the NAT device when the address and port-dependent filtering mode is used. This is the default mode, so datagram 4' is always allowed to pass.

 Copyright © Huawei Technologies Co., Ltd. 

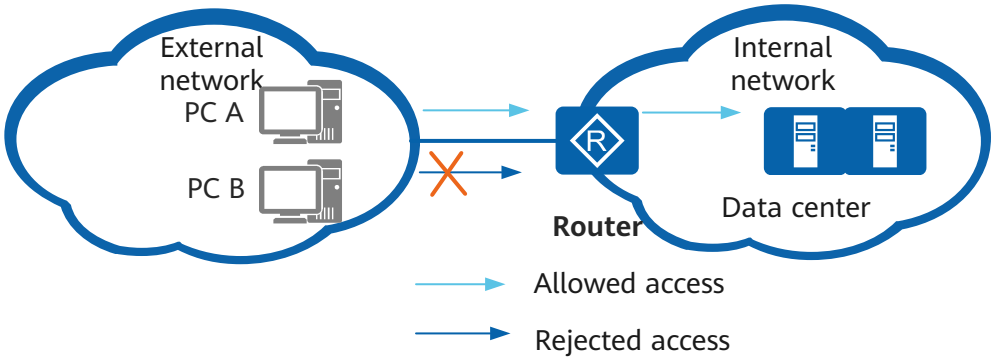
**Figure 5-10** Using ACL in NAT to filter traffic




## 5.3.8 Applying ACLs to the Firewall

The firewall is deployed between the internal and external networks to prevent the external network from attacking the internal network and protect the mainframes and key resources such as data on internal networks.

**Figure 5-11** Applying ACLs to the firewall




As shown in **Figure 5-11**, only PC A is allowed to access the data center on the internal network. You can deploy an ACL and configure the firewall on **Router** to meet the requirement.


Copyright © Huawei Technologies Co., Ltd.

# 5.4 Summary of ACL Configuration Tasks

The device supports the following types of ACLs: basic ACL, advanced ACL, Layer 2 ACL, user ACL, basic ACL6 and advanced ACL6.

Table 5-13 lists ACL configuration tasks. The configuration tasks can be performed in any sequence. You need to select at least one of them.

**Table 5-13** ACL configuration tasks

| Scenario | Description | Task |
| --- | --- | --- |
| Configure and apply a basic ACL. | A basic ACL defines rules to filter IPv4 packets based on information such as source IP addresses, fragment information, and time ranges.<br>If you only need to filter packets based on source IP addresses, you can configure a basic ACL. | **5.7.1 Configuring and Applying a Basic ACL** |
| Configure and apply an advanced ACL. | An advanced ACL defines rules to filter IPv4 packets based on source IP addresses, destination IP addresses, IP protocol types, TCP source/destination port numbers, UDP source/destination port numbers, fragment information, and time ranges.<br>Compared with a basic ACL, an advanced ACL is more accurate, flexible, and provides more functions. For example, if you want to filter packets based on source and destination IP addresses, configure an advanced ACL. | **5.7.2 Configuring and Applying an Advanced ACL** |


Copyright © Huawei Technologies Co., Ltd.

| Scenario | Description | Task |
| --- | --- | --- |
| Configure and apply a Layer 2 ACL. | A Layer 2 ACL defines rules to filter IPv4 and IPv6 packets based on Ethernet frame information, such as source Media Access Control (MAC) addresses, destination MAC addresses, VLANs, and Layer 2 protocol types.<br>If you only need to filter packets based on Layer 2 information, configure a Layer 2 ACL. | **5.7.3 Configuring and Applying a Layer 2 ACL** |
| Configure and apply a user ACL. | A user ACL defines rules to filter IPv4 packets based on the source IP addresses, destination IP addresses, IP protocol types, ICMP types, TCP source/destination port numbers, UDP source/destination port numbers, and time ranges.<br>To configure authentication-free rules for Portal users, configure a user ACL. | **5.7.4 Configuring and Applying a User ACL** |
| Configure and apply a basic ACL6. | A basic ACL6 defines rules to filter IPv6 packets based on information such as source IPv6 addresses, fragment information, and time ranges.<br>If you only need to filter packets based on source IPv6 addresses, you can configure a basic ACL6. | **5.7.5 Configuring and Applying a Basic ACL6** |


Copyright © Huawei Technologies Co., Ltd.

| Scenario | Description | Task |
| --- | --- | --- |
| Configure and apply an advanced ACL6. | An advanced ACL6 defines rules to filter IPv6 packets based on source IPv6 addresses, destination IPv6 addresses, IPv6 protocol types, TCP source/destination port numbers, UDP source/destination port numbers, fragment information, and time ranges.<br>Compared with a basic ACL6, an advanced ACL6 is more accurate, flexible, and provides more functions. For example, if you want to filter packets based on source and destination IPv6 addresses, configure an advanced ACL6. | **5.7.6 Configuring and Applying an Advanced ACL6** |

# 5.5 Licensing Requirements and Limitations for ACLs

## Involved Network Elements

Other network elements are not required.

## Licensing Requirements

ACL is a basic feature of the router and is not under license control.

## Feature Limitations

When deploying ACL on the router, pay attention to the following:

- The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support the ACL configured for Layer 2 forwarding traffic.

# 5.6 Default Settings for ACLs

**Table 5-14** describes default settings for ACLs.


Copyright © Huawei Technologies Co., Ltd.

**Table 5-14** Default settings for ACLs

| Parameter | Default Setting |
| --- | --- |
| Step | 5 |
| Matching order | Configuration order |

# 5.7 Configuring ACLs

## 5.7.1 Configuring and Applying a Basic ACL

### 5.7.1.1 (Optional) Creating a Time Range in Which an ACL Takes Effect

#### Context

By default, an ACL takes effect immediately after it is applied to a service module. If you want the ACL rules to take effect only in a certain period so that you can use **time-based ACL** to control services, you can define a time range and associate the time range with the ACL rules. By using a time-based ACL, an enterprise can forbid employees to access the Internet in work hours and restrict bandwidth for the bandwidth-consuming services such as P2P and downloading services in peak hours to avoid network congestion.

You can associate a time range with ACL rules in either of the following modes:

- Mode 1 - Periodic time range: defines a time range based on weeks. The associated ACL rules take effect at an interval of one week. For example, if the time range of ACL rules is 8:00-12:00 on Monday, the ACL rules take effect at 8:00-12:00 on every Monday.
- Mode 2 - Absolute time range: defines a time range from YYYY/MM/DD hh:mm to YYYY/MM/DD hh:mm. The associated ACL rules take effect only in this period.

NOTE

If the system time of a device is not synchronized with the network, the ACL rules cannot take effect in the associated time range. Therefore, it is recommended that you configure the Network Time Protocol (NTP) protocol on the device to synchronize system time. NTP ensures clock consistency on all devices on a network. For the NTP configuration, see Configuring Basic NTP Functions in the *Huawei AR Series Access Routers Configuration Guide - Device Management*.

#### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **time-range** *time-name* { *start-time* **to** *end-time* { *days* } &<1-7> | **from** *time1 date1* [ **to** *time2 date2* ] }

 Copyright © Huawei Technologies Co., Ltd. 

A time range is created.

By default, no time range is configured on a device.

You can specify multiple time ranges in the same *time-name* parameter. The device obtains the intersection of the configured periodic or absolute time ranges.

To delete a time range, see **Deleting a time range**.

**----End**

## Follow-up Procedure

After a time range is created, you need to create an ACL and configure the ACL rules to be associated with the time range. For the configuration of a basic ACL, see **5.7.1.3 Configuring a Basic ACL**.

## Configuration Tips

**Deleting a time range**

Before deleting a time range, you must delete the ACL rules associated with the time range or delete the ACL to which the ACL rules belong.

For example, ACL 2001 contains rule 5 and is associated with time range time1.

```
#
time-range time1 from 00:00 2014/1/1 to 23:59 2014/12/31
#
acl number 2001
 rule 5 permit time-range time1
#
```

Before deleting time1, delete rule 5 or ACL 2001.

- Delete rule 5, and then time1.

  ```
  <Huawei> system-view
  [Huawei] acl 2001
  [Huawei-acl-basic-2001] undo rule 5
  [Huawei-acl-basic-2001] quit
  [Huawei] undo time-range time1
  ```

- Delete ACL 2001, and then time1.

  ```
  <Huawei> system-view
  [Huawei] undo acl 2001
  [Huawei] undo time-range time1
  ```

# 5.7.1.2 (Optional) Configuring the Port Set

## Context

When configuring an advanced ACL with TCP or UDP protocol specified, you can bind a port set to the ACL to match the source and destination port numbers of packets. Specifying the source and destination port numbers in an advanced ACL is complex. You can specify the **port-set** *port-set-name* parameter in the **rule (advanced ACL view)** command to bind a port set to the ACL. This method is easier than specifying the **eq** *port*, **gt** *port*, **lt** *port*, or **range** *port-start port-end* parameter in the **rule (advanced ACL view)** command. In addition, you can use this method to specify the same port set for different ACL rules.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **ip port-set** *port-set-name* **protocol** { **tcp** | **udp** }

A port set is created and the port set view is displayed.

By default, no port set is created.

**Step 3** Run **port** [ *port-rule-id* ] { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }

Port rules are configured for the port set.

By default, no port rule is configured.

**----End**

## Follow-up Procedure

After a port set is configured, you need to create an advanced ACL and configure the ACL rules associated with the port set. For details about the advanced ACL configuration, see **5.7.2.2 Configuring an Advanced ACL**.

# 5.7.1.3 Configuring a Basic ACL

## Prerequisites

If you need to configure a time-based ACL, create a time range and associate the time range with the ACL rules. For details, see **5.7.1.1 (Optional) Creating a Time Range in Which an ACL Takes Effect**.

## Context

A basic ACL defines rules to filter IPv4 packets based on information such as source IP addresses, fragment information, and time ranges.

If you only need to filter packets based on source IP addresses, you can configure a basic ACL.

## Procedure

**Step 1** Run:

```
system-view
```

The system view is displayed.

**Step 2** Create a basic ACL. You can create a numbered or named ACL.

- Run the **acl** [ **number** ] *acl-number* [ **match-order** { **auto** | **config** } ] command to create a numbered basic ACL (2000-2999) and enter the basic ACL view.
- Run the **acl name** *acl-name* { **basic** | *acl-number* } [ **match-order** { **auto** | **config** } ] command to create a named basic ACL and enter the basic ACL view.

 Copyright © Huawei Technologies Co., Ltd. 

By default, no ACL exists on the device.

For details about the numbered and named ACLs, see **5.2.2 ACL Classification**.

If the **match-order** parameter is not specified when you create an ACL, the default match order **config** is used. For details about ACL match order, see **5.2.4 Matching Order**.

The default step of a created ACL is 5. If the default step cannot meet your ACL configuration requirements, you can change the step value. For details about the step, see **5.2.3 Step**; for configuration of the step, see **5.8.1 Adjusting the Step of ACL Rules**.

To delete an ACL that has taken effect, see **Deleting an ACL**.

**Step 3** (Optional) Run:

**description** *text*

A description is configured for the ACL.

By default, an ACL does not have a description.

The ACL description helps you understand and remember the functions or purpose of an ACL.

**Step 4** Run:

**rule** [ *rule-id* ] { **deny** | **permit** } [ **source** { *source-address source-wildcard* | **any** } | **vpn-instance** *vpn-instance-name* | [ **fragment** | **none-first-fragment** ] | **logging** | **time-range** *time-name* ] *

Rules are configured in the basic ACL.

In this example, only one permit or deny rule is configured. In actual configuration, you can configure multiple rules and decide the match order of the rules according to service requirements.

For details about the time range, source IP address and its wildcard mask, and IP fragment information, see **5.2.5 Matching Conditions**. **Configuring rules for a basic ACL** provides a rule configuration example.

**Step 5** (Optional) Run:

**rule** *rule-id* **description** *description*

A description is configured for the ACL rules.

By default, an ACL rule does not have a description.

The ACL rule description helps you understand and remember the functions or purpose of an ACL rule.

You can configure descriptions for only the rules existing on the device. That is, you cannot configure a description for a rule before creating the rule. If an ACL rule for which a description has been configured is deleted, the description is also deleted.

**----End**

## Configuration Tips

**Deleting an ACL**

 Copyright © Huawei Technologies Co., Ltd. 

To delete an ACL, run the **undo acl** { [ **number** ] *acl-number* | **all** } or **undo acl name** *acl-name* command in the system view. This command can delete an ACL.

**Configuring rules for a basic ACL**

- **Configuring a packet filtering rule based on the source IP address (host address)**

  To allow the packets from a host to pass, add a rule to an ACL. For example, to allow packets from host 192.168.1.3 to pass, create the following rule in ACL 2001.

  ```
  <Huawei> system-view
  [Huawei] acl 2001
  [Huawei-acl-basic-2001] rule permit source 192.168.1.3 0
  ```

- **Configuring a packet filtering rule based on the source IP address segment**

  To allow the packets from a host to pass and reject the packets from other hosts on the same network segment, configure rules in an ACL. For example, to allow the packets from host 192.168.1.3 to pass and reject the packets from other hosts on network segment 192.168.1.0/24, configure the following rules in ACL 2001 and set the description of ACL 2001 to Permit only 192.168.1.3 through.

  ```
  <Huawei> system-view
  [Huawei] acl 2001
  [Huawei-acl-basic-2001] rule permit source 192.168.1.3 0
  [Huawei-acl-basic-2001] rule deny source 192.168.1.0 0.0.0.255
  [Huawei-acl-basic-2001] description Permit only 192.168.1.3 through
  ```

- **Configuring a time-based ACL rule**

  Create a time range **working-time** (for example, 8:00-18:00 on Monday through Friday) and configure a rule in ACL **work-acl**. The rule rejects the packets from network segment 192.168.1.0/24 within the set **working-time**.

  ```
  <Huawei> system-view
  [Huawei] time-range working-time 8:00 to 18:00 working-day
  [Huawei] acl name work-acl basic
  [Huawei-acl-basic-work-acl] rule deny source 192.168.1.0 0.0.0.255 time-range working-time
  ```

- **Configuring a packet filtering rule based on the IP fragment information and source IP address segment**

  To reject the non-initial fragments from a network segment, configure a rule in an ACL. For example, to reject the non-initial fragments from network segment 192.168.1.0/24, configure the following rule in ACL 2001.

  ```
  <Huawei> system-view
  [Huawei] acl 2001
  [Huawei-acl-basic-2001] rule deny source 192.168.1.0 0.0.0.255 none-first-fragment
  ```

## 5.7.1.4 Applying a Basic ACL

## Context

After an ACL is configured, it must be applied to a service module so that the ACL rules can be delivered and take effect.

Usually, an ACL is applied to a traffic policy or simplified traffic policy so that the device can deliver ACL rules globally, or on an interface to filter packets to be forwarded. In addition, an ACL can be applied to the service modules such as Telnet, FTP, and routing.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Apply a basic ACL

Table 5-15 describes the application of a basic ACL.

**Table 5-15** Applying a basic ACL

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Filtering packets to be forwarded | The device filters received packets globally, or on an interface, and then discards, modifies priorities of, or redirects the filtered packets.<br>For example, you can use ACL to reduce the service level for the bandwidth-consuming services, such as P2P downloading and online video. When network congestion occurs, these packets are discarded first. | • Simplified traffic policy: See ACL-based Simplified Traffic Policy Configuration in *Huawei AR Series Access Routers Configuration Guide - QoS*.<br>• Traffic policy: See MQC Configuration in *Huawei AR Series Access Routers Configuration Guide - QoS*.<br>• Packet filtering firewall: See **6.7 Configuring the Packet Filtering Firewall** in *Huawei AR Series Access Routers Configuration Guide - Firewall*.<br>• Dynamic NAT: See Configuring Dynamic NAT in the *Huawei AR Series Access Routers Configuration Guide - IP Services*.<br>• NAT server: See Configuring an Internal NAT Server in the *Huawei AR Series Access Routers Configuration Guide - IP Services*. |

 Copyright © Huawei Technologies Co., Ltd. 

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Filtering packets to be sent to the CPU | If too many protocol packets are sent to the CPU, the CPU usage increases and CPU performance degrades. The device restricts the packets to be sent to the CPU.<br>For example, when a user sends a large number of ARP attack packets to the device, the CPU is busy and service is interrupted. You can apply an ACL to the local attack defense service, and add the user to the blacklist so that the CPU discards the packets from this user. | • Blacklist: See **8.4.2 Configuring a Blacklist** in Local Attack Defense Configuration. |


Copyright © Huawei Technologies Co., Ltd.

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Login control | The device controls access permission of users. Only authorized users can log in to the device, and other users cannot log in without permission. This ensures network security. | • Telnet: See Enabling the Telnet Server Function in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• FTP: See Managing Files When the Device Functions as an FTP Server in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• SFTP: See Managing Files When the Device Functions as an SFTP Server in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• TFTP: See Managing Files When the Device Functions as a TFTP Client in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• Web login: See (Optional) Configuring Web System Parameters in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• SNMP: See (Optional) Restricting Management Rights of the NMS (SNMPv1 and SNMPv2c) and (Optional) Restricting Management Rights of the NMS (SNMPv3) in *Huawei AR Series Access Routers Configuration Guide - Network Management and Monitoring*. |

 Copyright © Huawei Technologies Co., Ltd. 

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Route filtering | ACLs can be applied to various dynamic routing protocols to filter advertised and received routes and multicast groups.<br>For example, you can apply an ACL to a routing policy to prevent the device from sending routes of a network segment to the neighboring router. | • BGP: See Controlling the Advertisement of BGP Routes and Controlling the Receiving of BGP Routes in *Huawei AR Series Access Routers Configuration Guide - IP Unicast Routing*.<br>• IS-IS (IPv4): See Configuring IS-IS to Advertise Specified External Routes to an IS-IS Routing Domain and Adding Specified IS-IS Routes to the IP Routing Table in *Huawei AR Series Access Routers Configuration Guide - IP Unicast Routing*.<br>• OSPF: See Configuring OSPF to Filter the Received Routes, Configuring OSPF to Filter the Routes to Be Advertised, and (Optional) Configuring GR Session Parameters on the Helper in *Huawei AR Series Access Routers Configuration Guide - IP Unicast routing*.<br>• RIP: See Configuring RIP to Import Routes and Configuring RIP to Filter Received Routes in *Huawei AR Series Access Routers Configuration Guide - IP Unicast routing*.<br>• Multicast: See Filtering IGMP Messages Based on Source IP Addresses, Configuring a Multicast Group Policy, (Optional) Configuring the Range of Multicast Groups That an Interface Can Join, and (Optional) Configuring an SSM Group Policy in *Huawei AR Series Access* |

 Copyright © Huawei Technologies Co., Ltd. 

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| | | *Routers Configuration Guide - IP Multicast*. |

**----End**

### 5.7.1.5 Verifying a Basic ACL Configuration

#### Procedure

- Run the **display acl** { *acl-number* | **name** *acl-name* | **all** } command to check ACL configuration.
- Run the **display time-range** { **all** | *time-name* } command to view information about the time range.

**----End**

## 5.7.2 Configuring and Applying an Advanced ACL

### 5.7.2.1 (Optional) Creating a Time Range in Which an ACL Takes Effect

#### Context

For details, see **5.7.1.1 (Optional) Creating a Time Range in Which an ACL Takes Effect** in Configuring and Applying a Basic ACL.

### 5.7.2.2 Configuring an Advanced ACL

#### Pre-configuration Tasks

- If you need to configure a time-based ACL, create a time range and associate the time range with the ACL rules. For details, see **5.7.1.1 (Optional) Creating a Time Range in Which an ACL Takes Effect**.
- To apply an advanced ACL to a port set, create a port set and configure port rules for the port set first. For details, see **5.7.1.2 (Optional) Configuring the Port Set**.

#### Context

An advanced ACL defines rules to filter IPv4 packets based on source IP addresses, destination IP addresses, IP protocol types, TCP source/destination port numbers, UDP source/destination port numbers, fragment information, and time ranges.

Compared with a basic ACL, an advanced ACL is more accurate, flexible, and provides more functions. For example, if you want to filter packets based on source and destination IP addresses, configure an advanced ACL.


Copyright © Huawei Technologies Co., Ltd.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Create an advanced ACL. You can create a numbered or named ACL.

- Run the **acl** [ **number** ] *acl-number* [ **match-order** { **auto** | **config** } ] command to create a numbered advanced ACL (3000-3999) and enter the advanced ACL view.
- Run the **acl name** *acl-name* { **advance** | *acl-number* } [ **match-order** { **auto** | **config** } ] command to create a named advanced ACL and enter the advanced ACL view.

By default, no ACL exists on the device.

For details about the numbered and named ACLs, see **5.2.2 ACL Classification**.

If the **match-order** parameter is not specified when you create an ACL, the default match order **config** is used. For details about ACL match order, see **5.2.4 Matching Order**.

The default step of a created ACL is 5. If the default step cannot meet your ACL configuration requirements, you can change the step value. For details about the step, see **5.2.3 Step**; for configuration of the step, see **5.8.1 Adjusting the Step of ACL Rules**.

To delete an ACL that has taken effect, see **Deleting an ACL** in Configuring a Basic ACL.

**Step 3** (Optional) Run:

**description** *text*

A description is configured for the ACL.

By default, an ACL does not have a description.

The ACL description helps you understand and remember the functions or purpose of an ACL.

**Step 4** Configure rules for the advanced ACL.

You can configure advanced ACL rules according to the protocols carried by IP. The parameters vary according to the protocol type.

- When the ICMP protocol is used, run:

  **rule** [ *rule-id* ] { **deny** | **permit** } { *protocol-number* | **icmp** } [ **destination** { *destination-address destination-wildcard* | **any** } | **icmp-type** { *icmp-name* | *icmp-type icmp-code* } | **source** { *source-address source-wildcard* | **any** } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [ **dscp** *dscp* | [ **tos** *tos* | **precedence** *precedence* ] * ] | [ **fragment** | **none-first-fragment** ] | **vni** *vni-id* ] *

- When the TCP protocol is used, run:

  **rule** [ *rule-id* ] { **deny** | **permit** } { *protocol-number* | **tcp** } [ **destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt**

 Copyright © Huawei Technologies Co., Ltd. 

*port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** | **established** } * | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [ **dscp** *dscp* | [ **tos** *tos* | **precedence** *precedence* ] * ] | [ **fragment** | **none-first-fragment** ] | **vni** *vni-id* ] *

- When the UDP protocol is used, run:

  **rule** [ *rule-id* ] { **deny** | **permit** }{ *protocol-number* | **udp** } [ **destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [ **dscp** *dscp* | [ **tos** *tos* | **precedence** *precedence* ] * ] | [ **fragment** | **none-first-fragment** ] | **vni** *vni-id* ] *

- When GRE, IGMP, IPinIP, or OSPF is used, run:

  **rule** [ *rule-id* ] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ipinip** | **ospf** } [ **destination** { *destination-address destination-wildcard* | **any** } | **source** { *source-address source-wildcard* | **any** } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [ **dscp** *dscp* | [ **tos** *tos* | **precedence** *precedence* ] * ] | [ **fragment** | **none-first-fragment** ] | **vni** *vni-id* ] *

NOTE

To configure both the **precedence** *precedence* and **tos** *tos* parameters, set the two parameters consecutively in the command.

The **dscp** *dscp* and **precedence** *precedence* parameters cannot be set simultaneously for the same rule.

The **dscp** *dscp* and **tos** *tos* parameters cannot be set simultaneously for the same rule.

This parameter **vni** *vni-id* is valid only in the VXLAN scenario.

After the first rule is configured in an ACL, the device uses the step value as the number of this rule if the *rule-id* parameter is not specified. If the *rule-id* parameter is not specified for the later rules, the device uses the multiples of the next step of the last rule ID to number the rules. For example, if an ACL includes rule 5 and rule 7 and the step is 5, the system assigns 10 to a new rule without *rule-id* specified.

When you specify the **time-range** parameter to reference a validity time range to the ACL, if the specified *time-name* does not exit, the ACL does not take effect.

**Step 5** (Optional) Run:

**rule** *rule-id* **description** *description*

A description is configured for the ACL rules.

By default, an ACL rule does not have a description.

The ACL rule description helps you understand and remember the functions or purpose of an ACL rule.

You can configure descriptions for only the rules existing on the device. That is, you cannot configure a description for a rule before creating the rule. If an ACL rule for which a description has been configured is deleted, the description is also deleted.

**----End**

## Configuration Tips

**Configuring rules for an advanced ACL**

 Copyright © Huawei Technologies Co., Ltd. 

- **Configuring a packet filtering rule for ICMP protocol packets based on the source IP address (host address) and destination IP address segment**

  To allow the ICMP packets from a host that are destined for a network segment to pass, configure a rule in an ACL. For example, to allow the ICMP packets from host 192.168.1.3 that are destined for network segment 192.168.2.0/24 to pass, configure the following rule in ACL 3001.

```
<Huawei> system-view
[Huawei] acl 3001
[Huawei-acl-adv-3001] rule permit icmp source 192.168.1.3 0 destination 192.168.2.0 0.0.0.255
```

- **Configuring a packet filtering rule for TCP protocol packets based on the TCP destination port number, source IP address (host address), and destination IP address segment**

  To prohibit Telnet connections between the specified host and the hosts on a network segment, configure a rule in an advanced ACL. For example, to prohibit Telnet connections between host 192.168.1.3 and hosts on network segment 192.168.2.0/24, configure the following rule in the advanced ACL **deny-telnet**.

```
<Huawei> system-view
[Huawei] acl name deny-telnet
[Huawei-acl-adv-deny-telnet] rule deny tcp destination-port eq telnet source 192.168.1.3 0 destination 192.168.2.0 0.0.0.255
```

  To prohibit the specified hosts from accessing web pages (HTTP is used to access web pages, and TCP port number is 80), configure rules in an advanced ACL. For example, to prohibit hosts 192.168.1.3 and 192.168.1.4 from accessing web pages, configure the following rules in ACL **no-web** and set the description for the ACL to Web access restrictions.

```
<Huawei> system-view
[Huawei] acl name no-web
[Huawei-acl-adv-no-web] description Web access restrictions
[Huawei-acl-adv-no-web] rule deny tcp destination-port eq 80 source 192.168.1.3 0
[Huawei-acl-adv-no-web] rule deny tcp destination-port eq 80 source 192.168.1.4 0
```

- **Configuring a packet filtering rule for TCP packets based on the source IP address segment and TCP flags**

  To implement unidirectional access control on a network segment, configure rules in an ACL. For example, to implement unidirectional access control on network segment 192.168.2.0/24, configure the following rules in ACL 3002. In the following rules, the hosts on 192.168.2.0/24 can only respond to TCP handshake packets, but cannot send TCP handshake packets. Set the descriptions of the ACL rules to Allow the ACK TCP packets through, Allow the RST TCP packets through, and Do not Allow the other TCP packet through.

  To meet the preceding requirement, configure two permit rules to allow the packets with the ACK or RST field being 1 from 192.168.2.0/24 to pass, and then configure a deny rule to reject other TCP packets from this network segment.

```
<Huawei> system-view
[Huawei] acl 3002
[Huawei-acl-adv-3002] rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack
[Huawei-acl-adv-3002] display this   // If you do not specify an ID for a created rule, you can view the rule ID allocated by the system, and configure a description for the rule by specifying the rule ID.
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack          // The rule ID allocated by the system is 5.
#
return
[Huawei-acl-adv-3002] rule 5 description Allow the ACK TCP packets through
[Huawei-acl-adv-3002] rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Huawei-acl-adv-3002] display this
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack syn
 rule 5 description Allow the ACK TCP packets through
 rule 10 deny tcp source 192.168.2.0 0.0.0.255 tcp-flag rst       // The rule ID allocated by the system is
10.
#
return
[Huawei-acl-adv-3002] rule 10 description Allow the RST TCP packets through
[Huawei-acl-adv-3002] rule deny tcp source 192.168.2.0 0.0.0.255
[Huawei-acl-adv-3002] display this
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack syn
 rule 5 description Allow the ACK TCP packets through
 rule 10 deny tcp source 192.168.2.0 0.0.0.255 tcp-flag rst
 rule 10 description Allow the RST TCP packets through
 rule 15 deny tcp source 192.168.2.0 0.0.0.255       //  The rule ID allocated by the system is 15.
#
return
[Huawei-acl-adv-3002] rule 15 description Do not Allow the other TCP packet through
```

- **Configuring a time-based ACL rule**

  For details, see **Configuring a time-based ACL rule** in Configuring a Basic ACL.

- **Configuring a packet filtering rule based on the IP fragment information and source IP address segment**

  For details, see **Configuring a packet filtering rule based on the IP fragment information and source IP address segment** in Configuring a Basic ACL.

### 5.7.2.3 Applying an Advanced ACL

## Context

After an ACL is configured, it must be applied to a service module so that the ACL rules can be delivered and take effect.

Usually, an ACL is applied to a traffic policy or simplified traffic policy so that the device can deliver ACL rules globally, or on an interface to filter packets to be forwarded. In addition, an ACL can be applied to the service modules such as FTP and multicast.

## Procedure

**Step 1** Apply an advanced ACL

**Table 5-16** describes the application of an advanced ACL.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 5-16** Applying an advanced ACL

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Filtering packets to be forwarded | The device filters received packets globally, or on an interface, and then discards, modifies priorities of, or redirects the filtered packets.<br>For example, you can use ACL to reduce the service level for the bandwidth-consuming services, such as P2P downloading and online video. When network congestion occurs, these packets are discarded first. | • Simplified traffic policy: See ACL-based Simplified Traffic Policy Configuration in *Huawei AR Series Access Routers Configuration Guide - QoS*.<br>• Traffic policy: See MQC Configuration in *Huawei AR Series Access Routers Configuration Guide - QoS*.<br>• Packet filtering firewall: See **6.7 Configuring the Packet Filtering Firewall** in *Huawei AR Series Access Routers Configuration Guide - Firewall*.<br>• Dynamic NAT: See Configuring Dynamic NAT in the *Huawei AR Series Access Routers Configuration Guide - IP Services*.<br>• NAT server: See Configuring an Internal NAT Server in the *Huawei AR Series Access Routers Configuration Guide - IP Services*. |
| Filtering packets to be sent to the CPU | If too many protocol packets are sent to the CPU, the CPU usage increases and CPU performance degrades. The device restricts the packets to be sent to the CPU.<br>For example, when a user sends a large number of ARP attack packets to the device, the CPU is busy and service is interrupted. You can apply an ACL to the local attack defense service, and add the user to the blacklist so that the CPU discards the packets from this user. | Blacklist: See **8.4.2 Configuring a Blacklist** in Local Attack Defense Configuration. |


Copyright © Huawei Technologies Co., Ltd.

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Login control | The device controls access permission of users. Only authorized users can log in to the device, and other users cannot log in without permission. This ensures network security. | • Telnet: See Enabling the Telnet Server Function in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• FTP: See Managing Files When the Device Functions as an FTP Server in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• SFTP: See Managing Files When the Device Functions as an SFTP Server in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*. |
| Route filtering | An ACL can be applied to the multicast protocol to filter multicast groups.<br>For example, the ACL and IGMP snooping functions can be used together to prevent hosts in a VLAN from joining a multicast group. | Multicast: See Filtering IGMP Messages Based on Source IP Addresses, Configuring a Multicast Group Policy, and (Optional) Configuring the Range of Multicast Groups That an Interface Can Join in *Huawei AR Series Access Routers Configuration Guide - IP Multicast*. |

**----End**

### 5.7.2.4 Verifying an Advanced ACL Configuration

### Procedure

- Run the **display acl** { *acl-number* | **name** *acl-name* | **all** } command to check ACL configuration.
- Run the **display time-range** { **all** | *time-name* } command to view information about the time range.

**----End**

## 5.7.3 Configuring and Applying a Layer 2 ACL

 Copyright © Huawei Technologies Co., Ltd. 

### 5.7.3.1 (Optional) Creating a Time Range in Which an ACL Takes Effect

#### Context

For details, see **5.7.1.1 (Optional) Creating a Time Range in Which an ACL Takes Effect** in Configuring and Applying a Basic ACL.

### 5.7.3.2 Configuring a Layer 2 ACL

#### Pre-configuration Tasks

If you need to configure a time-based ACL, create a time range and associate the time range with the ACL rules. For details, see **5.7.1.1 (Optional) Creating a Time Range in Which an ACL Takes Effect**.

#### Context

A Layer 2 ACL defines rules to filter IPv4 and IPv6 packets based on Ethernet frame information, such as source Media Access Control (MAC) addresses, destination MAC addresses, VLANs, and Layer 2 protocol types.

If you only need to filter packets based on Layer 2 information, configure a Layer 2 ACL.

#### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Create a Layer 2 ACL. You can create a numbered or named ACL.

- Run the **acl** [ **number** ] *acl-number* [ **match-order** { **auto** | **config** } ] command to create a numbered Layer 2 ACL (4000-4999) and enter the Layer 2 ACL view.
- Run the **acl name** *acl-name* { **link** | *acl-number* } [ **match-order** { **auto** | **config** } ] command to create a named Layer 2 ACL and enter the Layer 2 ACL view.

By default, no ACL exists on the device.

For details about the numbered and named ACLs, see **5.2.2 ACL Classification**.

If the **match-order** parameter is not specified when you create an ACL, the default match order **config** is used. For details about ACL match order, see **5.2.4 Matching Order**.

The default step of a created ACL is 5. If the default step cannot meet your ACL configuration requirements, you can change the step value. For details about the step, see **5.2.3 Step**; for configuration of the step, see **5.8.1 Adjusting the Step of ACL Rules**.

To delete an ACL that has taken effect, see **Deleting an ACL** in Configuring a Basic ACL.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 3** (Optional) Run:

**description** *text*

A description is configured for the ACL.

By default, an ACL does not have a description.

The ACL description helps you understand and remember the functions or purpose of an ACL.

**Step 4** Run **rule** [ *rule-id* ] { **permit** | **deny** } [ **l2-protocol** *type-value* [ *type-mask* ] | **destination-mac** *dest-mac-address* [ *dest-mac-mask* ] | **source-mac** *source-mac-address* [ *source-mac-mask* ] | **vlan-id** *vlan-id* [ *vlan-id-mask* ] | **8021p** *802.1p-value* | **time-range** *time-name* ] *

Rules are configured in the Layer 2 ACL.

In this example, only one permit or deny rule is configured. In actual configuration, you can configure multiple rules and decide the match order of the rules according to service requirements.

For details about the time range, source/destination MAC addresses and their wildcard masks, VLAN IDs and their masks, see **5.2.5 Matching Conditions**. **Configuring rules for a Layer 2 ACL** provides a rule configuration example.

**Step 5** (Optional) Run:

**rule** *rule-id* **description** *description*

A description is configured for the ACL rules.

By default, an ACL rule does not have a description.

The ACL rule description helps you understand and remember the functions or purpose of an ACL rule.

You can configure descriptions for only the rules existing on the device. That is, you cannot configure a description for a rule before creating the rule. If an ACL rule for which a description has been configured is deleted, the description is also deleted.

**----End**

## Configuration Tips

**Configuring rules for a Layer 2 ACL**

- **Configuring packet filtering rules based on the source MAC address, destination MAC address, and Layer 2 protocol types**

  To allow the ARP packets with the specified destination and source MAC addresses and Layer 2 protocol type to pass, configure a rule in a Layer 2 ACL. For example, to allow the ARP packets with destination MAC address 0000-0000-0001, source MAC address 0000-0000-0002, and Layer 2 protocol type 0x0806 to pass, configure the following rule in ACL 4001.

  ```
  <Huawei> system-view
  [Huawei] acl 4001
  [Huawei-acl-L2-4001] rule permit destination-mac 0000-0000-0001 source-mac 0000-0000-0002 l2-protocol 0x0806
  ```

  To reject the PPPoE packets with the specified Layer 2 protocol type, configure a rule in a Layer 2 ACL. To reject the PPPoE packets with Layer 2 protocol type 0x8863, configure the following rule in ACL 4001.

 Copyright © Huawei Technologies Co., Ltd. 

```
<Huawei> system-view
[Huawei] acl 4001
[Huawei-acl-L2-4001] rule deny l2-protocol 0x8863
```

- **Configuring a packet filtering rule based on the source MAC address segment and inner VLAN IDs**

  To reject the packets from the specified MAC address segments in a VLAN, configure a rule in a Layer 2 ACL. For example, to reject the packets from source MAC address segment 00e0-fc01-0000 to 00e0-fc01-ffff in VLAN 10, configure the following rule in Layer 2 ACL **deny-vlan10-mac**.

```
<Huawei> system-view
[Huawei] acl name deny-vlan10-mac link
[Huawei-acl-L2-deny-vlan10-mac] rule deny vlan-id 10 source-mac 00e0-fc01-0000 ffff-ffff-0000
```

- **Configuring a time-based ACL rule**

  For details, see **Configuring a time-based ACL rule** in Configuring a Basic ACL.

## 5.7.3.3 Applying a Layer 2 ACL

### Context

After an ACL is configured, it must be applied to a service module so that the ACL rules can be delivered and take effect.

Usually, an ACL is applied to a traffic policy or simplified traffic policy so that the device can deliver ACL rules globally, or on an interface to filter packets to be forwarded. In addition, an ACL can be applied to the service modules such as local attack defense.

### Procedure

**Step 1** Apply a Layer 2 ACL.

**Table 5-17** describes the application of a Layer 2 ACL.

**Table 5-17** Applying a Layer 2 ACL

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Filtering packets to be forwarded | The device filters received packets globally, or on an interface, and then discards, modifies priorities of, or redirects the filtered packets.<br>For example, you can use ACL to reduce the service level for the bandwidth-consuming services, such as P2P downloading and online video. When network congestion occurs, these packets are discarded first. | • Simplified traffic policy: See ACL-based Simplified Traffic Policy Configuration in *Huawei AR Series Access Routers Configuration Guide - QoS*.<br>• Traffic policy: See MQC Configuration in *Huawei AR Series Access Routers Configuration Guide - QoS*.<br>• Packet filtering firewall: See **6.7 Configuring the Packet Filtering Firewall** in *Huawei AR Series Access Routers Configuration Guide - Firewall*.<br>• Dynamic NAT: See Configuring Dynamic NAT in the *Huawei AR Series Access Routers Configuration Guide - IP Services*.<br>• NAT server: See Configuring an Internal NAT Server in the *Huawei AR Series Access Routers Configuration Guide - IP Services*. |
| Filtering packets to be sent to the CPU | If too many protocol packets are sent to the CPU, the CPU usage increases and CPU performance degrades. The device restricts the packets to be sent to the CPU.<br>For example, when a user sends a large number of ARP attack packets to the device, the CPU is busy and service is interrupted. You can apply an ACL to the local attack defense service, and add the user to the blacklist so that the CPU discards the packets from this user. | Blacklist: See **8.4.2 Configuring a Blacklist** in Local Attack Defense Configuration. |

 Copyright © Huawei Technologies Co., Ltd. 

**----End**

### 5.7.3.4 Verifying a Layer 2 ACL Configuration

#### Procedure

- Run the **display acl** { *acl-number* | **name** *acl-name* | **all** } command to check ACL configuration.
- Run the **display time-range** { **all** | *time-name* } command to view information about the time range.

**----End**

## 5.7.4 Configuring and Applying a User ACL

### 5.7.4.1 (Optional) Creating a Time Range in Which an ACL Takes Effect

#### Context

For details, see **5.7.1.1 (Optional) Creating a Time Range in Which an ACL Takes Effect** in Configuring and Applying a Basic ACL.

### 5.7.4.2 Configuring a User ACL

#### Context

A user ACL defines rules to filter IPv4 packets based on the source IP addresses, destination IP addresses, IP protocol types, ICMP types, TCP source/destination port numbers, UDP source/destination port numbers, and time ranges.

To configure authentication-free rules for Portal users, configure a user ACL.

#### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Create a user ACL. Only numbered ACL is supported.

- Run the **acl** [ **number** ] *acl-number* [ **match-order** { **auto** | **config** } ] command to create a numbered user ACL (6000-6031) and enter the user ACL view.

By default, no ACL exists on the device.

For details about the numbered and named ACLs, see **5.2.2 ACL Classification**.

 Copyright © Huawei Technologies Co., Ltd. 

If the **match-order** parameter is not specified when you create an ACL, the default match order **config** is used. For details about ACL match order, see **5.2.4 Matching Order**.

The default step of a created ACL is 5. If the default step cannot meet your ACL configuration requirements, you can change the step value. For details about the step, see **5.2.3 Step**; for configuration of the step, see **5.8.1 Adjusting the Step of ACL Rules**.

To delete an ACL that has taken effect, see **Deleting an ACL** in Configuring a Basic ACL.

**Step 3** (Optional) Run:

**description** *text*

A description is configured for the ACL.

By default, an ACL does not have a description.

The ACL description helps you understand and remember the functions or purpose of an ACL.

**Step 4** Configure user ACL rules.

You can configure the user ACL rules according to the protocol types of IP packets. The parameters vary according to the protocol types.

- When the protocol is ICMP, run:

  **rule** [ *rule-id* ] { **deny** | **permit** } { *protocol-number* | **icmp** } [ **destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **icmp-type** { *icmp-name* | *icmp-type icmp-code* } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | [ **dscp** *dscp* | [ **tos** *tos* | **precedence** *precedence* ] * ] | **fragment** ] *

- When the protocol is TCP, run:

  **rule** [ *rule-id* ] { **deny** | **permit** } { *protocol-number* | **tcp** } [ **destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }
  | **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | [ **dscp** *dscp* | [ **tos** *tos* | **precedence** *precedence* ] * ] | **fragment** ] *

- When the protocol is UDP, run:

  **rule** [ *rule-id* ] { **deny** | **permit** } { *protocol-number* | **udp** } [ **destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | [ **dscp** *dscp* | [ **tos** *tos* | **precedence** *precedence* ] * ] | **fragment** ] *

- When the protocol is GRE, IGMP, IP, IPINIP, or OSPF, run:

  **rule** [ *rule-id* ] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [ **destination** { *destination-address*
  *destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | [ **dscp** *dscp* | [ **tos** *tos* | **precedence** *precedence* ] * ] | **fragment** ] *

In this example, only one permit or deny rule is configured. In actual configuration, you can configure multiple rules and decide the match order of the rules according to service requirements.

A rule configuration example is provided in **Configuring user ACL rules**.

**Step 5** (Optional) Run:

**rule** *rule-id* **description** *description*

 Copyright © Huawei Technologies Co., Ltd. 

A description is configured for the ACL rules.

By default, an ACL rule does not have a description.

The ACL rule description helps you understand and remember the functions or purpose of an ACL rule.

You can configure descriptions for only the rules existing on the device. That is, you cannot configure a description for a rule before creating the rule. If an ACL rule for which a description has been configured is deleted, the description is also deleted.

**----End**

## Configuration Tips

**Configuring user ACL rules**

- **Configuring a packet filtering rule based on the destination IP address**

  Configure a rule in ACL 6000 to allow all Portal users to access network segment 10.1.1.1/24 without authentication.

  ```
  <Huawei> system-view
  [Huawei] acl 6000
  [Huawei-acl-ucl-6000] rule permit ip destination 10.1.1.1 255.255.255.0
  ```

- **Configuring a time-based ACL rule**

  For details, see **Configuring a time-based ACL rule** in Configuring a Basic ACL.

## 5.7.4.3 Applying a User ACL

## Context

After an ACL is configured, it must be applied to a service module so that the ACL rules can be delivered and take effect.

The user ACL can only be applied to the Portal authentication in NAC. After Portal authentication is configured and authentication-free rules are configured for the Portal authentication users, certain users can access the specified network resources without authentication or upon an authentication failure.

## Procedure

**Step 1** Apply a user ACL.

**Table 5-18** describes the application of a user ACL.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 5-18** Applying a user ACL

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Filtering packets to be forwarded | After a user ACL is bound to the authentication-free rules for Portal authentication users, certain users can access the specified network resources without authentication or upon an authentication failure. | NAC: See **3.6.3.5.1 (Optional) Configuring Authorization Information for Authentication-free Users**. |

**----End**

### 5.7.4.4 Verifying a User ACL Configuration

#### Procedure

- Run the **display acl** { *acl-number* | **name** *acl-name* | **all** } command to check ACL configuration.
- Run the **display time-range** { **all** | *time-name* } command to view information about the time range.

**----End**

## 5.7.5 Configuring and Applying a Basic ACL6

### 5.7.5.1 (Optional) Creating a Time Range in Which an ACL6 Takes Effect

#### Context

The time range configurations of ACL6 and ACL are the same. For details, see **5.7.1.1 (Optional) Creating a Time Range in Which an ACL Takes Effect** in Configuring and Applying a Basic ACL.

### 5.7.5.2 Configuring a Basic ACL6

#### Pre-configuration Tasks

If you need to configure a time-based ACL6, create a time range and associate the time range with the ACL6 rules. For details, see **5.7.5.1 (Optional) Creating a Time Range in Which an ACL6 Takes Effect**.

#### Context

A basic ACL6 defines rules to filter IPv6 packets based on information such as source IPv6 addresses, fragment information, and time ranges.


Copyright © Huawei Technologies Co., Ltd.

If you only need to filter packets based on source IPv6 addresses, you can configure a basic ACL6.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Create a basic ACL6. You can create a numbered or named ACL.

- Run the **acl ipv6** [ **number** ] *acl6-number* [ **match-order** { **auto** | **config** } ] command to create a numbered basic ACL6 (2000-2999) and enter the basic ACL6 view.
- Run the **acl ipv6 name** *acl6-name* { **basic** | *acl6-number* } [ **match-order** { **auto** | **config** } ] command to create a named basic ACL6 and enter the basic ACL6 view.

By default, no ACL6 exists on the device.

The functions of numbered and named ACL6 are the same as the functions of numbered and named ACL. For details, see **5.2.2 ACL Classification**.

If the **match-order** parameter is not specified when you create an ACL6, the default match order **config** is used. The match order of ACL6 is the same as that of ACL. For details, see **5.2.4 Matching Order**.

To delete an ACL6 that has taken effect, see **Deleting ACL6**.

**Step 3** Run **rule** [ *rule-id* ] { **deny** | **permit** } [ [ **fragment** | **none-first-fragment** ] | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **logging** | **time-range** *time-name* ] *

Rules are configured in the basic ACL6.

In this example, only one permit or deny rule is configured. In actual configuration, you can configure multiple rules and decide the match order of the rules according to service requirements.

**Configuring rules for the basic ACL6** provides a rule configuration example.

**Step 4** (Optional) Run:

**rule** *rule-id* **description** *description*

A description is configured for the ACL rules.

By default, an ACL rule does not have a description.

The ACL rule description helps you understand and remember the functions or purpose of an ACL rule.

You can configure descriptions for only the rules existing on the device. That is, you cannot configure a description for a rule before creating the rule. If an ACL rule for which a description has been configured is deleted, the description is also deleted.

**----End**


Copyright © Huawei Technologies Co., Ltd.

## Configuration Tips

**Deleting ACL6**

Run the **undo acl ipv6** { **all** | [ **number** ] *acl6-number* } or **undo acl ipv6 name** *acl6-name* command in the system view to delete an ACL6. This command can delete an ACL6.

**Configuring rules for the basic ACL6**

- **Configuring a packet filtering rule based on the source IPv6 address (host address)**

  Configure a rule in ACL6 2001 to allow the packets from host fc00:1::1/128 to pass.

  ```
  <Huawei> system-view
  [Huawei] acl ipv6 2001
  [Huawei-acl6-basic-2001] rule permit source fc00:1::1 128
  ```

- **Configuring a packet filtering rule based on the source IPv6 address segment**

  Configure a rule in ACL6 2001 to allow the packets from host fc00:1::1/128 to pass and reject the packets from other hosts on network segment fc00:1::/64.

  ```
  <Huawei> system-view
  [Huawei] acl ipv6 2001
  [Huawei-acl6-basic-2001] rule permit source fc00:1::1 128
  [Huawei-acl6-basic-2001] rule deny source fc00:1:: 64
  ```

- **Configuring a time-based ACL6 rule**

  For details, see **Configuring a time-based ACL rule** in Configuring a Basic ACL.

- **Configuring a packet filtering rule based on the IP fragment information and source IP address segment**

  For details, see **Configuring a packet filtering rule based on the IP fragment information and source IP address segment** in Configuring a Basic ACL.

## 5.7.5.3 Applying a Basic ACL6

## Context

After an ACL6 is configured, it must be applied to a service module so that the ACL6 rules can be delivered and take effect.

Usually, an ACL6 is applied to a traffic policy or simplified traffic policy so that the device can deliver ACL rules globally, or on an interface to filter packets to be forwarded. In addition, an ACL6 can be applied to the service modules such as Telnet, FTP, and routing.

## Procedure

**Step 1** Apply a basic ACL6.

**Table 5-19** describes the application of a basic ACL6.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 5-19** Applying a basic ACL6

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Filtering packets to be forwarded | The device filters received packets globally, or on an interface, and then discards, modifies priorities of, or redirects the filtered packets.<br>For example, you can use ACL6 to reduce the service level for the bandwidth-consuming services, such as P2P downloading and online video. When network congestion occurs, these packets are discarded first. | • Simplified traffic policy: See ACL-based Simplified Traffic Policy Configuration in *Huawei AR Series Access Routers Configuration Guide - QoS*.<br>• Traffic policy: See MQC Configuration in *Huawei AR Series Access Routers Configuration Guide - QoS*.<br>• Packet filtering firewall: See **6.7 Configuring the Packet Filtering Firewall** in *Huawei AR Series Access Routers Configuration Guide - Firewall*.<br>• Dynamic NAT: See Configuring Dynamic NAT in the *Huawei AR Series Access Routers Configuration Guide - IP Services*.<br>• NAT server: See Configuring an Internal NAT Server in the *Huawei AR Series Access Routers Configuration Guide - IP Services*. |

 Copyright © Huawei Technologies Co., Ltd. 

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Login control | The device controls access permission of users. Only authorized users can log in to the device, and other users cannot log in without permission. This ensures network security.<br>For example, only the administrator is allowed to log in to the device. You can apply an ACL6 to the Telnet service and specify the hosts that are allowed to log in to the device. | • Telnet: See Enabling the Telnet Server Function in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• FTP: See Managing Files When the Device Functions as an FTP Server in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• SFTP: See Managing Files When the Device Functions as an SFTP Server in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• SNMP: See (Optional) Restricting Management Rights of the NMS (SNMPv1 and SNMPv2c) and (Optional) Restricting Management Rights of the NMS (SNMPv3) in *Huawei AR Series Access Routers Configuration Guide - Network Management and Monitoring*. |


Copyright © Huawei Technologies Co., Ltd.

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Route filtering | ACLs can be applied to various dynamic routing protocols to filter advertised and received routes and multicast groups.<br>For example, you can apply an ACL to a routing policy to prevent the device from sending routes of a network segment to the neighboring router. | • IS-IS (IPv6): See Configuring IS-IS to Advertise Specified External Routes to an IS-IS Routing Domain and Adding Specified IS-IS Routes to the IP Routing Table in *Huawei AR Series Access Routers Configuration Guide - IP Unicast Routing*.<br>• OSPFv3: See Configuring OSPFv3 to Filter the Received Routes, Configuring OSPFv3 to Import External Routes, and Enabling the Helper of OSPFv3 GR in *Huawei AR Series Access Routers Configuration Guide - IP Unicast Routing*.<br>• RIPng: See Configuring a RIPng Process to Import External Routes and Controlling the Receiving of RIPng Routes in *Huawei AR Series Access Routers Configuration Guide - IP Unicast routing*.<br>• Multicast: See Filtering IGMP Messages Based on Source IP Addresses, Configuring a Multicast Group Policy, (Optional) Configuring the Range of Multicast Groups That an Interface Can Join, and (Optional) Configuring an SSM Group Policy in *Huawei AR Series Access Routers Configuration Guide - IP Multicast*. |

**----End**

## 5.7.5.4 Verifying a Basic ACL6 Configuration


Copyright © Huawei Technologies Co., Ltd.

### Procedure

- Run the **display acl ipv6** { *acl6-number* | **name** *acl6-name* | **all** } command to check ACL6 configuration.
- Run the **display time-range** { **all** | *time-name* } command to view information about the time range.

**----End**

## 5.7.6 Configuring and Applying an Advanced ACL6

### 5.7.6.1 (Optional) Creating a Time Range in Which an ACL6 Takes Effect

### Context

The time range configurations of ACL6 and ACL are the same. For details, see **5.7.1.1 (Optional) Creating a Time Range in Which an ACL Takes Effect** in Configuring and Applying a Basic ACL.

### 5.7.6.2 Configuring an Advanced ACL6

### Prerequisites

If you need to configure a time-based ACL6, create a time range and associate the time range with the ACL6 rules. For details, see **5.7.5.1 (Optional) Creating a Time Range in Which an ACL6 Takes Effect**.

### Context

An advanced ACL6 defines rules to filter IPv6 packets based on source IPv6 addresses, destination IPv6 addresses, IPv6 protocol types, TCP source/destination port numbers, UDP source/destination port numbers, fragment information, and time ranges.

Compared with a basic ACL6, an advanced ACL6 is more accurate, flexible, and provides more functions. For example, if you want to filter packets based on source and destination IPv6 addresses, configure an advanced ACL6.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Create an advanced ACL6. You can create a numbered or named ACL.

- Run the **acl ipv6** [ **number** ] *acl6-number* [ **match-order** { **auto** | **config** } ] command to create a numbered advanced ACL6 (3000-3999) and enter the advanced ACL6 view.
- Run the **acl ipv6 name** *acl6-name* { **advance** | *acl6-number* } [ **match-order** { **auto** | **config** } ] command to create a named advanced ACL6 and enter the advanced ACL6 view.

 Copyright © Huawei Technologies Co., Ltd. 

By default, no ACL exists on the device.

The functions of numbered and named ACL6 are the same as the functions of numbered and named ACL. For details, see **5.2.2 ACL Classification**.

If the **match-order** parameter is not specified when you create an ACL6, the default match order **config** is used. The match order of ACL6 is the same as that of ACL. For details, see **5.2.4 Matching Order**.

To delete an ACL that has taken effect, see **Deleting an ACL** in Configuring a Basic ACL6.

**Step 3** Configure rules for the advanced ACL6.

You can configure advanced ACL6 rules according to the protocols carried by IP. The parameters vary according to the protocol types.

- When the TCP protocol is used, run:

  **rule** [ *rule-id* ] { **deny** | **permit** } { *protocol-number* | **tcp** } [ **destination** { [ **pd** *prefix* ] *destination-ipv6-address prefix-length* | [ **pd** *prefix* ] *destination-ipv6-address/prefix-length* | **any** | **pd** *destination-dhcpv6-prefix* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **dscp** *dscp* | **precedence** *precedence* | **source** { [ **pd** *prefix* ] *source-ipv6-address prefix-length* | [ **pd** *prefix* ] *source-ipv6-address/prefix-length* | **any** | **pd** *source-dhcpv6-prefix* } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** | **established** } * | **logging** | **time-range** *time-name* | **tos** *tos* ] *
- When the UDP protocol is used, run:

  **rule** [ *rule-id* ] { **deny** | **permit** } { *protocol-number* | **udp** } [ **destination** { [ **pd** *prefix* ] *destination-ipv6-address prefix-length* | [ **pd** *prefix* ] *destination-ipv6-address/prefix-length* | **any** | **pd** *destination-dhcpv6-prefix* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **dscp** *dscp* | **precedence** *precedence* | **source** { [ **pd** *prefix* ] *source-ipv6-address prefix-length* | [ **pd** *prefix* ] *source-ipv6-address/prefix-length* | **any** | **pd** *source-dhcpv6-prefix* } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **logging** | **time-range** *time-name* | **tos** *tos* ] *
- When the ICMPv6 protocol is used, run:

  **rule** [ *rule-id* ] { **deny** | **permit** } { *protocol-number* | **icmpv6** } [ **destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | **any** } | **dscp** *dscp* | **icmp6-type** { *icmp6-type-name* | *icmp6-type icmp6-code* } | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **logging** | **time-range** *time-name* | **tos** *tos* ] *
- When the IPv6 protocol is used, run:

  **rule** [ *rule-id* ] { **deny** | **permit** } { *protocol-number* | **ipv6** } [ **destination** { [ **pd** *prefix* ] *destination-ipv6-address prefix-length* | [ **pd** *prefix* ] *destination-ipv6-address/prefix-length* | **any** | **pd** *destination-dhcpv6-prefix* } | **dscp** *dscp* | [ **fragment** | **none-first-fragment** ] | **precedence** *precedence* | **source** { [ **pd** *prefix* ] *source-ipv6-address prefix-length* | [ **pd** *prefix* ] *source-ipv6-address/prefix-length* | **any** | **pd** *source-dhcpv6-prefix* } | **logging** | **time-range** *time-name* | **tos** *tos* ] *
- When other protocols are used, run:

 Copyright © Huawei Technologies Co., Ltd. 

**rule** [ *rule-id* ] { **deny** | **permit** } { *protocol-number* | **gre** | **ospf** } [ **destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | **any** } | **dscp** *dscp* | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **logging** | **time-range** *time-name* | **tos** *tos* ] *

In this example, only one permit or deny rule is configured. In actual configuration, you can configure multiple rules and decide the match order of the rules according to service requirements.

**Configuring rules for the advanced ACL6** provides a rule configuration example.

**Step 4** (Optional) Run:

**rule** *rule-id* **description** *description*

A description is configured for the ACL rules.

By default, an ACL rule does not have a description.

The ACL rule description helps you understand and remember the functions or purpose of an ACL rule.

You can configure descriptions for only the rules existing on the device. That is, you cannot configure a description for a rule before creating the rule. If an ACL rule for which a description has been configured is deleted, the description is also deleted.

**----End**

## Configuration Tips

**Configuring rules for the advanced ACL6**

- **Configuring a packet filtering rule for ICMPv6 protocol packets based on source IPv6 address (host address) and destination IPv6 address segment**

  Configure a rule in ACL6 3001 to allow the ICMPv6 packets from fc00:1::1 and destined for network segment fc00:2::/64 to pass.

  ```
  <Huawei> system-view
  [Huawei] acl ipv6 3001
  [Huawei-acl6-adv-3001] rule permit icmpv6 source fc00:1::1 128 destination fc00:2:: 64
  ```

- **Configuring a packet filtering rule for TCP protocol packets based on the TCP destination port number, source IPv6 address (host address), and destination IPv6 address segment**

  Configure a rule in the advanced ACL6 deny-telnet to forbid Telnet connections between the host fc00:1::3 and hosts on network segment fc00:2::/64.

  ```
  <Huawei> system-view
  [Huawei] acl ipv6 name deny-telnet
  [Huawei-acl6-adv-deny-telnet] rule deny tcp destination-port eq telnet source fc00:1::3 128 destination fc00:2:: 64
  ```

  Configure a rule in the advanced ACL6 no-web to forbid hosts fc00:1::3 and fc00:1::4 from accessing web pages (HTTP is used to access web pages, and TCP port number is 80).

  ```
  <Huawei> system-view
  [Huawei] acl ipv6 name no-web
  [Huawei-acl6-adv-no-web] rule deny tcp destination-port eq 80 source fc00:1::3 128
  [Huawei-acl6-adv-no-web] rule deny tcp destination-port eq 80 source fc00:1::4 128
  ```

- **Configuring a time-based ACL6 rule**

 Copyright © Huawei Technologies Co., Ltd. 

For details, see **Configuring a time-based ACL rule** in Configuring a Basic ACL.

- **Configuring a packet filtering rule based on the IP fragment information and source IP address segment**

  For details, see **Configuring a packet filtering rule based on the IP fragment information and source IP address segment** in Configuring a Basic ACL.

### 5.7.6.3 Applying an Advanced ACL6

## Context

After an ACL6 is configured, it must be applied to a service module so that the ACL6 rules can be delivered and take effect.

Usually, an ACL6 is applied to a traffic policy or simplified traffic policy so that the device can deliver ACL rules globally, or on an interface to filter packets to be forwarded. In addition, an ACL6 can be applied to the service modules such as FTP and multicast.

## Procedure

**Step 1** Apply an advanced ACL6.

**Table 5-20** describes the application of an advanced ACL6.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 5-20** Applying an advanced ACL6

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Filtering packets to be forwarded | The device filters received packets globally, or on an interface, and then discards, modifies priorities of, or redirects the filtered packets.<br>For example, you can use ACL6 to reduce the service level for the bandwidth-consuming services, such as P2P downloading and online video. When network congestion occurs, these packets are discarded first. | • Simplified traffic policy: See ACL-based Simplified Traffic Policy Configuration in *Huawei AR Series Access Routers Configuration Guide - QoS*.<br>• Traffic policy: See MQC Configuration in *Huawei AR Series Access Routers Configuration Guide - QoS*.<br>• Packet filtering firewall: See **6.7 Configuring the Packet Filtering Firewall** in *Huawei AR Series Access Routers Configuration Guide - Firewall*.<br>• Dynamic NAT: See Configuring Dynamic NAT in the *Huawei AR Series Access Routers Configuration Guide - IP Services*.<br>• NAT server: See Configuring an Internal NAT Server in the *Huawei AR Series Access Routers Configuration Guide - IP Services*.<br>**NOTE**<br>Only the packet filtering firewall service supports the **rule (advanced ACL6 view)** command to configure ACL6 rules to match the IPv6 address, which is assigned based on the IPv6 address prefix obtained by a DHCPv6 client, as the source or destination IP address of packets. In the same ACL6 rule, **destination pd** *destination-dhcpv6-prefix* and **source pd** *source-dhcpv6-prefix* parameters cannot be configured simultaneously. |

 Copyright © Huawei Technologies Co., Ltd. 

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Login control | The device controls access permission of users. Only authorized users can log in to the device, and other users cannot log in without permission. This ensures network security.<br>For example, only the administrator is allowed to log in to the device. You can apply an ACL6 to the Telnet service and specify the hosts that are allowed to log in to the device. | • Telnet: See Enabling the Telnet Server Function in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• FTP: See Managing Files When the Device Functions as an FTP Server in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• SFTP: See Managing Files When the Device Functions as an SFTP Server in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*. |
| Route filtering | An ACL6 can be applied to the multicast protocol to filter multicast groups.<br>For example, the ACL6 and MLD snooping functions can be used together to prevent hosts in a VLAN from joining a multicast group. | Multicast: See Configuring a Multicast Group Policy in Configuring the MLD Snooping Policy, Configuring a Multicast Group Policy in Configuring the IGMP Snooping Policy, Filtering IGMP Messages Based on Source IP Addresses and (Optional) Configuring the Range of Multicast Groups That an Interface Can Join in *Huawei AR Series Access Routers Configuration Guide - IP Multicast*. |

**----End**

## 5.7.6.4 Verifying an Advanced ACL6 Configuration

## Procedure

- Run the **display acl ipv6** { *acl6-number* | **name** *acl6-name* | **all** } command to check ACL6 configuration.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **display time-range** { **all** | *time-name* } command to view information about the time range.

**----End**

# 5.8 Maintaining ACLs

## 5.8.1 Adjusting the Step of ACL Rules

### Context

During routine maintenance, you may need to add rules to an ACL to meet new service requirements. If the default step 5 is used (the system allocates 5, 10, 15... as rule IDs), you can insert only four rules (rules 6, 7, 8, and 9) between neighboring rules. If you need to insert more than 4 rules between neighboring rules, increase the step to a value greater than 6. Then the system reallocates IDs (6, 12, 18...) to the rules, and you can insert more than four rules (rules 7, 8, 9, 10, and 11) between neighboring rules.

For details about the step, see **5.2.3 Step**.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** You can create a numbered or named ACL.

- Run the **acl** [ **number** ] *acl-number* [ **match-order** { **auto** | **config** } ] command to create a numbered ACL (2000-4999 or 6000-6031) and enter the ACL view.
- Run the **acl name** *acl-name* [ **advance** | **basic** | **link** | *acl-number* ] [ **match-order** { **auto** | **config** } ] command to create a named ACL and enter the ACL view.

By default, no ACL exists on the device.

For details about the numbered and named ACLs, see **5.2.2 ACL Classification**.

**Step 3** Run **step** *step*

The step is set.

The default step is 5.

**----End**

## 5.8.2 Displaying ACL Resources

### Context

If the device prompts that an ACL fails to be applied, the available ACL resources in the system may be insufficient.

 Copyright © Huawei Technologies Co., Ltd. 

You can view ACL resource usage in the system to check whether the ACL resources have been used up.

## Procedure

- Run the **display acl resource** [ **slot** *slot-id* ] command in any view to check information about ACL resources.

  If the values of Remaining is not 0, idle ACL resources exist on the device.

**----End**

# 5.8.3 Optimizing ACL Resources

If the system prompts that ACL resources are insufficient when you configure a service that occupies ACL resources, the use of ACL resources on the device needs to be optimized. In addition to deleting unneeded services to release ACL resources, you can adjust the ACL application range or combine ACL rules for the services. The traffic policy service is used as an example here (For the ACL resource calculation method for traffic policy, see MQC Configuration - Configuration Notes in *Huawei AR Series Access Routers Configuration Guide - QoS*.)

For example, you have run the **if-match acl** { *acl-number* | *acl-name* } command to configure 1K rules and applied the traffic policy associated with the ACL to the **outbound** direction of 8 interfaces. This configuration requires 8K ACL resources, which exceed the maximum outbound ACL resources (7K) supported by the device; therefore, the configuration fails. You can use either of the following methods to optimize ACL resources:

- Method 1: Adjust ACL application range.

  If the interfaces to which the traffic policy is applied belong to the same VLAN or some of the interfaces belong to the same VLAN (the interfaces without traffic policy configured are not in this VLAN), you can apply the ACL to the VLANs (for example, VLAN 10 and VLAN 20) to which the interfaces belong. After the ACL application range is adjusted, the number of occupied ACL resources is 2K (1K rules x 2 VLANs).

- Method 2: Combine ACL rules.

  Find out the common matching conditions in the ACL rules and relationships between the rules.

  For example, the following content is included in 1K ACL rules:

```
#
acl number 3009
 rule 1 permit ip source 10.1.1.1 0 destination 10.10.1.1 0
 rule 2 permit ip source 10.1.1.2 0 destination 10.10.1.1 0
 rule 3 permit ip source 10.1.1.3 0 destination 10.10.1.1 0
 rule 4 permit ip source 10.1.1.4 0 destination 10.10.1.1 0
 ...
 rule 255 permit ip source 10.1.1.255 0 destination 10.10.1.1 0
 rule 256 permit ip source 10.1.2.1 0 destination 10.10.1.1 0
 ...
 rule 510 permit ip source 10.1.2.255 0 destination 10.10.1.1 0
 ...
 rule 801 deny tcp destination-port eq www      //Port 80
 rule 802 deny tcp destination-port eq 81
 rule 803 deny tcp destination-port eq 82
 ...
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 rule 830 deny tcp destination-port eq pop2  //Port 109
 rule 831 deny tcp destination-port eq pop3  //Port 110
 ...
 rule 1000 xxx
#
```

Rules 1 through 510 use source and destination IP addresses as matching conditions. Source IP addresses are all IP addresses on network segments 10.1.1.0/24 and 10.1.2.0/24. Therefore, rules 1 through 510 can be combined into the following two rules by using the IP address wildcard mask.

```
#
acl number 3009
 rule 1 permit ip source 10.1.1.0 0.0.0.255 destination 10.10.1.1 0
 rule 2 permit ip source 10.1.2.0 0.0.0.255 destination 10.10.1.1 0
 ...
#
```

After combination, rules 1 through 510 are reduced to 492 rules. The number of occupied ACL resources is reduced to 3936 (492 rules x 8 interfaces), which is lower than the upper limit of ACL resources.

## 5.8.4 Clearing ACL Statistics

### Context

**NOTICE**

The deleted ACL statistics cannot be restored. Exercise caution when you run the command.

### Procedure

- Run the **reset acl counter** { **name** *acl-name* | *acl-number* | **all** } command in the user view to clear ACL statistics.
- Run the **reset acl ipv6 counter** { **name** *acl6-name* | *acl6-number* | **all** } command in the user view to clear ACL6 statistics.

**----End**

# 5.9 Configuration Examples for ACLs

## 5.9.1 Example for Using Basic ACLs to Restrict FTP Access Rights

### Networking Requirements

As shown in **Figure 5-12**, the Router functions as an FTP server. The requirements are as follows:

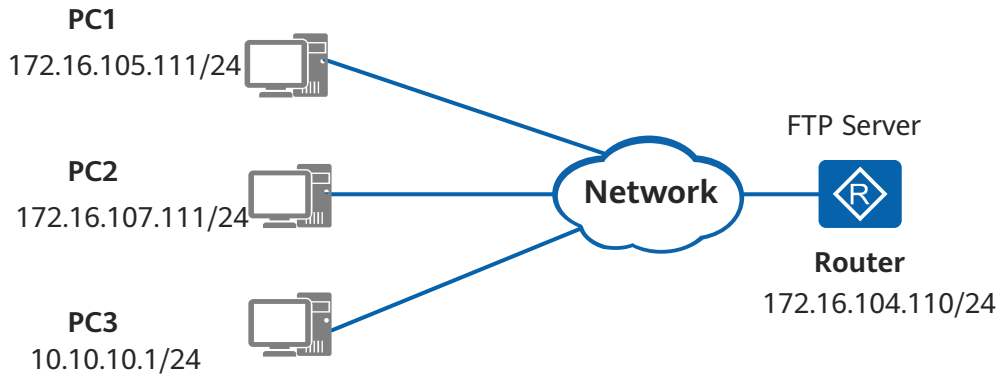
- All the users on subnet 1 (172.16.105.0/24) are allowed to access the FTP server anytime.

 Copyright © Huawei Technologies Co., Ltd. 

- All the users on subnet 2 (172.16.107.0/24) are allowed to access the FTP server only at the specified period of time.
- Other users are not allowed to access the FTP server.

The routes between the Router and subnets are reachable. You need to configure the Router to limit user access to the FTP server.

**Figure 5-12** Using basic ACLs to restrict FTP access rights




## Configuration Roadmap

The following configurations are performed on the Router. The configuration roadmap is as follows:

1. Configure time ranges and ACLs so that the device can filter user packets to control FTP access rights of different users.
2. Configure basic FTP functions.
3. Apply the ACL to the FTP module to make the ACL take effect.

## Procedure

**Step 1** Configure time ranges.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] time-range ftp-access from 0:0 2014/1/1 to 23:59 2014/12/31
[Router] time-range ftp-access 14:00 to 18:00 off-day
```

**Step 2** Configure a basic ACL.

```
[Router] acl number 2001
[Router-acl-basic-2001] rule permit source 172.16.105.0 0.0.0.255
[Router-acl-basic-2001] rule permit source 172.16.107.0 0.0.0.255 time-range ftp-access
[Router-acl-basic-2001] rule deny source any
[Router-acl-basic-2001] quit
```

**Step 3** Configure basic FTP functions.

```
[Router] ftp server enable
[Router] aaa
[Router-aaa] local-user huawei password irreversible-cipher SetUesrPasswd@123
[Router-aaa] local-user huawei privilege level 15
[Router-aaa] local-user huawei service-type ftp
[Router-aaa] local-user huawei ftp-directory flash:
[Router-aaa] quit
```

 Copyright © Huawei Technologies Co., Ltd. 

**Step 4** Configure access permissions on the FTP server.

```
[Router] ftp acl 2001
```

**Step 5** Verify the configuration.

Run the **ftp 172.16.104.110** command on PC1 (172.16.105.111/24) in subnet 1. PC1 can connect to the FTP server.

Run the **ftp 172.16.104.110** command on PC2 (172.16.107.111/24) in subnet 2 on Monday in 2014. PC2 cannot connect to the FTP server. Run the **ftp 172.16.104.110** command on PC2 (172.16.107.111/24) in subnet 2 at 15:00 on Saturday in 2014. PC2 can connect to the FTP server.

Run the **ftp 172.16.104.110** command on PC3 (10.10.10.1/24). PC3 cannot connect to the FTP server.

**----End**

## Configuration Files

Router configuration file

```
#
sysname Router
#
time-range ftp-access 14:00 to 18:00 off-day
time-range ftp-access from 00:00 2014/1/1 to 23:59 2014/12/31
#
acl number 2001
 rule 5 permit source 172.16.105.0 0.0.0.255
 rule 10 permit source 172.16.107.0 0.0.0.255 time-range ftp-access
 rule 15 deny
#
aaa
 local-user huawei password irreversible-cipher %^%#a/sUWg/.p1*))=~SWzIRS0N",`&aS%'7X).m=o[PkQcv"!!
TTQOI~Z)C'1<9%^%#
 local-user huawei privilege level 15
 local-user huawei ftp-directory flash:
 local-user huawei service-type ftp
#
 ftp server enable
 ftp acl 2001
#
return
```

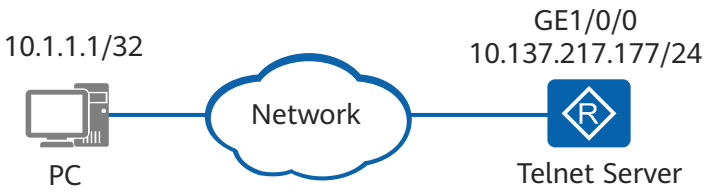
# 5.9.2 Example for Using Basic ACLs to Control Telnet Login Rights

## Networking Requirements

As shown in **Figure 5-13**, the PC and the server (Huawei device) are reachable to each other. To implement easy remote configuration and management of the device, configure AAA authentication for Telnet users on the server and configure an ACL security policy that allows only users in compliance with the security policy to log in to the device.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 5-13** Networking diagram for Configuring a Security Policy to Limit Telnet Login




NOTE

The Telnet protocol poses a security risk, and therefore the STelnet V2 protocol is recommended.

## Configuration Roadmap

The following configurations are performed on the Router. The configuration roadmap is as follows:

1. Configure the Telnet login mode to implement remote network device maintenance.
2. Configure an ACL security policy to ensure that only users in compliance with the security policy can log in to the device.
3. Configure the administrator's user name and password and the AAA authentication mode to ensure that only users passing the authentication can log in to the device.

## Procedure

**Step 1** Set the server listening port number and enable the server function.

```
<Huawei> system-view
[Huawei] sysname Telnet Server
[Telnet Server] telnet server enable
[Telnet Server] telnet server port 1025
```

**Step 2** Set the VTY user interface parameters.

# Set the maximum number of VTY user interfaces.

```
[Telnet Server] user-interface maximum-vty 8
```

# Set the IP address of the device to which the user is allowed to log in.

```
[Telnet Server] acl 2001
[Telnet Server-acl-basic-2001] rule permit source 10.1.1.1 0
[Telnet Server-acl-basic-2001] quit
[Telnet Server] user-interface vty 0 7
[Telnet Server-ui-vty0-7] acl 2001 inbound
```

# Configure the terminal attributes of the VTY user interface.

```
[Telnet Server-ui-vty0-7] shell
[Telnet Server-ui-vty0-7] idle-timeout 20
[Telnet Server-ui-vty0-7] screen-length 30
[Telnet Server-ui-vty0-7] history-command max-size 20
```

# Configure the user authentication mode of the VTY user interface.

 Copyright © Huawei Technologies Co., Ltd. 

```
[Telnet Server-ui-vty0-7] authentication-mode aaa
[Telnet Server-ui-vty0-7] quit
```

**Step 3** Configure the login user information.

# Configure the login authentication mode.

```
[Telnet Server] aaa
[Telnet Server-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
[Telnet Server-aaa] local-user admin1234 service-type telnet
[Telnet Server-aaa] local-user admin1234 privilege level 3
[Telnet Server-aaa] quit
```

**Step 4** Configure the client login.

Enter commands at the command line prompt to log in to the device through Telnet.

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177 1025
```

Press **Enter**, and enter the user name and password in the login window. If the authentication is successful, the command line prompt of the user view is displayed. The user view configuration environment is displayed.

```
Login authentication

Username:admin1234
Password:
<Telnet Server>
```

**----End**

## Configuration Files

Telnet server configuration file

```
#
 sysname Telnet Server
#
acl number 2001
 rule 5 permit source 10.1.1.1 0
#
aaa
 local-user admin1234 password irreversible-cipher %^%#*~Br";[g6Pv5Zf>$~{hY+N!`{$<[Y{;l02P)B,EBz\1FN!c
+%^%#
 local-user admin1234 privilege level 3
 local-user admin1234 service-type telnet
#
 telnet server enable
 telnet server port 1025
#
user-interface maximum-vty 8
user-interface vty 0 7
 acl 2001 inbound
 authentication-mode aaa
 history-command max-size 20
 idle-timeout 20 0
 screen-length 30
#
return
```

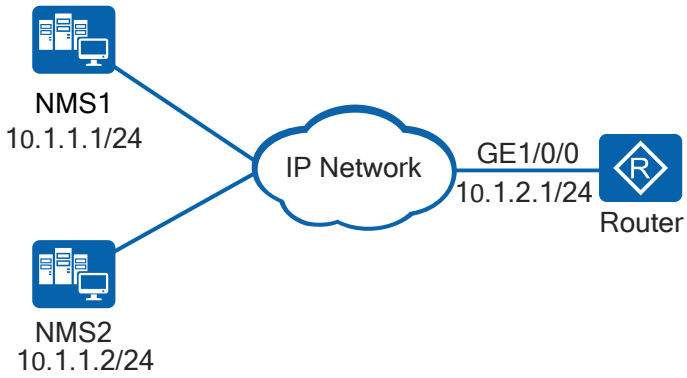
# 5.9.3 Example for Applying Basic ACLs to SNMP to Filter NMSs

 Copyright © Huawei Technologies Co., Ltd. 

## Networking Requirements

As shown in **Figure 5-14**, two NMSs are available on the network to monitor network devices. The network size is small and the network has a high security level. Therefore, the administrator requires that only the trusted NMS (NMS2) manage network devices and the Router use SNMPv1 to communicate with the NMS. Invalid NMSs cannot manage the Router. According to service requirements, the administrator allows the NMS to manage only the objects DNS, and the administrator should be able to locate and rectify faults quickly through the NMS.

**Figure 5-14** Applying basic ACLs to SNMP to filter NMSs




## Configuration Roadmap

The following configurations are performed on the Router. The configuration roadmap is as follows:

1. Configure SNMPv1 on the router.
2. Configure ACLs, MIB view, and community name to control the access rights of NMSs. The NMS2 can only manage the objects on Router except RMON, and NMS1 cannot manage the Router.
3. Configure the trap function on the router to send alarms generated on the router to NMS2. Only modules that are enabled by default can send alarms, which helps locate alarms and prevent unwanted alarms.
4. Configure contact information about the router administrator to quickly troubleshoot faults when the router fails.
5. Configure the NM station (only NMS2).

## Procedure

**Step 1** Configure the IP address and route on the router and ensure the route between the device and the NMS is reachable.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 10.1.2.1 24
[Router-GigabitEthernet1/0/0] quit
[Router] ospf
[Router-ospf-1] area 0
[Router-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router-ospf-1-area-0.0.0.0] quit
[Router-ospf-1] quit
```

**Step 2** Enable the SNMP agent.

```
[Router] snmp-agent
```

**Step 3** Configure SNMPv1 on the Router.

```
[Router] snmp-agent sys-info version v1
```

**Step 4** Configure access rights of the NM station.

# Configure ACLs, enable NMS2 to manage the Router, and disable NMS1 from managing the Router.

```
[Router] acl 2001
[Router-acl-basic-2001] rule 5 permit source 10.1.1.2 0.0.0.0
[Router-acl-basic-2001] rule 6 deny source 10.1.1.1 0.0.0.0
[Router-acl-basic-2001] quit
```

# Configure a MIB view.

```
[Router] snmp-agent mib-view iso include iso
```

# Configure the source interface from which traps are sent.

```
[Router] snmp-agent trap source gigabitethernet 1/0/0
```

# Configure an SNMP community name and reference the configured ACLs and the MIB view.

```
[Router] snmp-agent community write adminnms2 mib-view iso acl 2001
```

**Step 5** Configure the trap function.

```
[Router] snmp-agent target-host trap-paramsname trapnms2 v1 securityname adminnms2
[Router] snmp-agent target-host trap-hostname nms2 address 10.1.1.2 trap-paramsname trapnms2
[Router] snmp-agent trap queue-size 200
[Router] snmp-agent trap life 60
[Router] snmp-agent trap enable
```

**Step 6** Configure contact information about the device administrator.

```
[Router] snmp-agent sys-info contact call Operator at 010-12345678
```

**Step 7** Configure the NM station (NMS2).

Set read and write community names on the NMS that uses SNMPv1. For configurations of the NMS, refer to related configuration guides.

**NOTE**

Authentication parameter configuration of the NMS must be the same as that of the device. If the authentication parameter configuration of the NMS is different from that of the device, the NMS cannot manage the device. If only the write community name is configured on the device, the read and write community names on the NMS must be the same as the write community name configured on the device.

**Step 8** Verify the configuration.

After the configuration is complete, run the following commands to verify that the configurations have taken effect.

# Check the configured SNMP version.

```
<Router> display snmp-agent sys-info version
  SNMP version running in the system:
        SNMPv1
```

 Copyright © Huawei Technologies Co., Ltd. 

# View the community names.

```
<Router> display snmp-agent community write
  Community name: %^%#$X!5#d+t+OJOXL1[{O2!&Fe&0UZv'@a;R/`Y+kK$4BUGFe)&2YLuM/kMF!
HPG5Mzz3DXe2&F%^%#

  Storage type: nonVolatile
  View name: iso
  Acl: 2001

  Total number is 1
```

# Check the configuration of ACLs.

```
<Router> display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5
 rule 5 permit source 10.1.1.2 0
 rule 6 deny source 10.1.1.1 0
```

# Display the MIB view.

```
<Router> display snmp-agent mib-view iso
  View name: iso
  MIB subtree: iso
  Subtree mask:
  Storage type: nonVolatile
  View type: included
  View status: active
```

# Check the target host for alarms.

```
<Router> display snmp-agent target-host
  Traphost list:
  Target host name: nms2
  Traphost address: 10.1.1.2
  Traphost portnumber: 162
  Target host parameter: trapnms2

  Total number is 1

  Parameter list trap target host:
  Parameter name of the target host: trapnms2
  Message mode of the target host: SNMPV1
  Trap version of the target host: v1
  Security name of the target host: %^%#_=XqAFC_94uCS,3'<gYC*ZU6%^%#

  Total number is 1
```

# Check contact information about the device administrator.

```
<Router> display snmp-agent sys-info contact
  The contact person for this managed node:
        call Operator at 010-12345678
```

**----End**

## Configuration Files

Configuration file of the Router

```
#
 sysname Router
#
acl number 2001
 rule 5 permit source 10.1.1.2 0
 rule 6 deny source 10.1.1.1 0
#
interface GigabitEthernet1/0/0
```

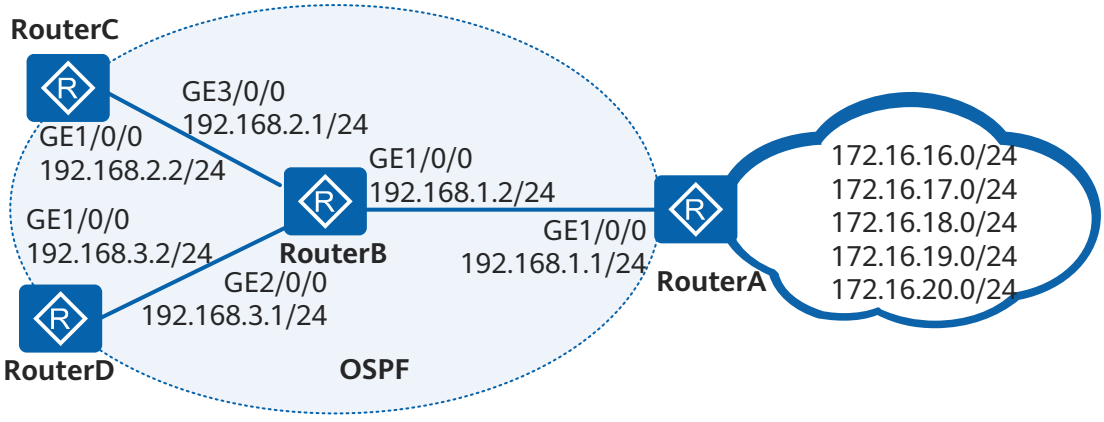
```
 ip address 10.1.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
#
 snmp-agent local-engineid 800007DB03548998F3A458
 snmp-agent community write %^%#$X!5#d+t+OJOXL1[{O2!&Fe&0UZv'@a;R/`Y+kK$4BUGFe)&2YLuM/kMF!
HPG5Mzz3DXe2&F%^%# mib-view iso acl 2001
 snmp-agent sys-info contact call Operator at 010-12345678
 snmp-agent sys-info version v1
 snmp-agent target-host trap-hostname nms2 address 10.1.1.2 udp-port 162 trap-paramsname trapnms2
 snmp-agent target-host trap-paramsname trapnms2 v1 securityname %^%#_=XqAFC_94uCS,
3'<gYC*ZU6%^%#
 snmp-agent mib-view iso include iso
 snmp-agent trap source gigabitethernet 1/0/0
 snmp-agent trap enable
 snmp-agent trap queue-size 200
 snmp-agent trap life 60
 snmp-agent
#
return
```

# 5.9.4 Example for Using Basic ACLs to Filter OSPF Routes

## Networking Requirements

Figure 5-15 shows how on an OSPF network, RouterA receives routes from the Internet and provides these routes for the OSPF network. A user wants devices on the OSPF network to access only the network segments 172.16.17.0/24, 172.16.18.0/24, and 172.16.19.0/24, and RouterC to access only the network segment 172.16.18.0/24.

**Figure 5-15** Networking diagram for filtering received and advertised routes




## Configuration Roadmap

The following configurations are performed on the Router. The configuration roadmap is as follows:

1. Configure an ACL on RouterA so that RouterA advertises only the 172.16.17.0/24, 172.16.18.0/24, and 172.16.19.0/24 routes to RouterB. In this

 Copyright © Huawei Technologies Co., Ltd. 

situation, the OSPF network can access only 172.16.17.0/24, 172.16.18.0/24, and 172.16.19.0/24.

2. Configure an ACL on RouterC so that RouterC receives only the 172.16.18.0/24 routes. In this situation, the network connected to RouterC can access only the network segments 172.16.18.0/24.

## Procedure

**Step 1** Assign an IP address to each interface.

# Configure IP addresses for all interfaces of RouterA.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 255.255.255.0
[RouterA-GigabitEthernet1/0/0] quit
```

The configurations of RouterB, RouterC and RouterD are similar to the configuration of RouterA, and are not mentioned here.

**Step 2** Configure basic OSPF functions.

# Configure RouterA.

```
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

# Configure RouterB.

```
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
```

# Configure RouterC.

```
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

# Configure RouterD.

```
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] quit
```

**Step 3** Configure five static routes on RouterA and import these routes into OSPF.

```
[RouterA] ip route-static 172.16.16.0 24 NULL 0
[RouterA] ip route-static 172.16.17.0 24 NULL 0
[RouterA] ip route-static 172.16.18.0 24 NULL 0
[RouterA] ip route-static 172.16.19.0 24 NULL 0
[RouterA] ip route-static 172.16.20.0 24 NULL 0
[RouterA] ospf
[RouterA-ospf-1] import-route static
[RouterA-ospf-1] quit
```

 Copyright © Huawei Technologies Co., Ltd. 

# Check the IP routing table on RouterB. You can see that the five static routes are imported into OSPF.

```
[RouterB] display ip routing-table
Route Flags:
R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 18        Routes : 18

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    172.16.16.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
    172.16.17.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
    172.16.18.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
    172.16.19.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
    172.16.20.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
   192.168.1.0/24   Direct  0    0           D   192.168.1.2     GigabitEthernet1/0/0
   192.168.1.2/32   Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
 192.168.1.255/32   Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
   192.168.2.0/24   Direct  0    0           D   192.168.2.1     GigabitEthernet3/0/0
   192.168.2.1/32   Direct  0    0           D   127.0.0.1       GigabitEthernet3/0/0
 192.168.2.255/32   Direct  0    0           D   127.0.0.1       GigabitEthernet3/0/0
   192.168.3.0/24   Direct  0    0           D   192.168.3.1     GigabitEthernet2/0/0
   192.168.3.1/32   Direct  0    0           D   127.0.0.1       GigabitEthernet2/0/0
 192.168.3.255/32   Direct  0    0           D   127.0.0.1       GigabitEthernet2/0/0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

**Step 4** Configure a route advertisement policy.

# Configure ACL 2002 on RouterA to allow only 172.16.17.0/24, 172.16.18.0/24, and 172.16.19.0/24 to pass.

```
[RouterA] acl number 2002
[RouterA-acl-basic-2002] rule permit source 172.16.17.0 0.0.0.255
[RouterA-acl-basic-2002] rule permit source 172.16.18.0 0.0.0.255
[RouterA-acl-basic-2002] rule permit source 172.16.19.0 0.0.0.255
[RouterA-acl-basic-2002] quit
```

# Configure a route advertisement policy on RouterA and associate ACL 2002 with the policy to filter routes.

```
[RouterA] ospf
[RouterA-ospf-1] filter-policy 2002 export static
[RouterA-ospf-1] quit
```

# View the IP routing table on RouterB. RouterB has received only the three routes defined in ACL 2002.

```
[RouterB] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 16        Routes : 16

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   172.16.17.0/24   O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
   172.16.18.0/24   O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
   172.16.19.0/24   O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
   192.168.1.0/24   Direct  0    0           D   192.168.1.2     GigabitEthernet1/0/0
   192.168.1.2/32   Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
 192.168.1.255/32   Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
```

 Copyright © Huawei Technologies Co., Ltd. 

```
  192.168.2.0/24  Direct  0    0           D   192.168.2.1     GigabitEthernet3/0/0
  192.168.2.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet3/0/0
192.168.2.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet3/0/0
  192.168.3.0/24  Direct  0    0           D   192.168.3.1     GigabitEthernet2/0/0
  192.168.3.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet2/0/0
192.168.3.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet2/0/0
255.255.255.255/32  Direct  0    0         D   127.0.0.1       InLoopBack0
```

**Step 5** Configure a route receiving policy.

# Configure ACL 2003 on RouterC to allow only 172.16.18.0/24 to pass.

```
[RouterC] acl number 2003
[RouterC-acl-basic-2003] rule permit source 172.16.18.0 0.0.0.255
[RouterC-acl-basic-2003] quit
```

# Configure a route receiving policy on RouterC and associate ACL 2003 with the policy to filter routes.

```
[RouterC] ospf
[RouterC-ospf-1] filter-policy 2003 import
[RouterC-ospf-1] quit
```

# View the IP routing table on RouterC. RouterC has received only the route defined in ACL 2003.

```
[RouterC] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 8        Routes : 8

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   172.16.18.0/24  O_ASE   150  1           D   192.168.2.1     GigabitEthernet1/0/0
   192.168.2.0/24  Direct  0    0           D   192.168.2.2     GigabitEthernet1/0/0
   192.168.2.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
 192.168.2.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
255.255.255.255/32  Direct  0    0         D   127.0.0.1       InLoopBack0
```

**----End**

## Configuration Files

- RouterA configuration file

```
#
sysname RouterA
#
acl number 2002
 rule 5 permit source 172.16.17.0 0.0.0.255
 rule 10 permit source 172.16.18.0 0.0.0.255
 rule 15 permit source 172.16.19.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
#
ospf 1
 filter-policy 2002 export static
 import-route static
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
ip route-static 172.16.16.0 255.255.255.0 NULL0
ip route-static 172.16.17.0 255.255.255.0 NULL0
ip route-static 172.16.18.0 255.255.255.0 NULL0
```

 Copyright © Huawei Technologies Co., Ltd. 

```
ip route-static 172.16.19.0 255.255.255.0 NULL0
ip route-static 172.16.20.0 255.255.255.0 NULL0
#
return
```

- RouterB configuration file

```
#
sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet3/0/0
 ip address 192.168.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
return
```

- RouterC configuration file

```
#
sysname RouterC
#
acl number 2003
 rule 5 permit source 172.16.18.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.2 255.255.255.0
#
ospf 1
 filter-policy 2003 import
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
#
 ip ip-prefix in index 10 permit 172.16.18.0 24
#
return
```

- RouterD configuration file

```
#
 sysname RouterD
#
interface GigabitEthernet1/0/0
 ip address 192.168.3.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
#
return
```

# 5.9.5 Example for Configuring a Basic ACL in URPF to Prevent Source IP Address Spoofing Attacks

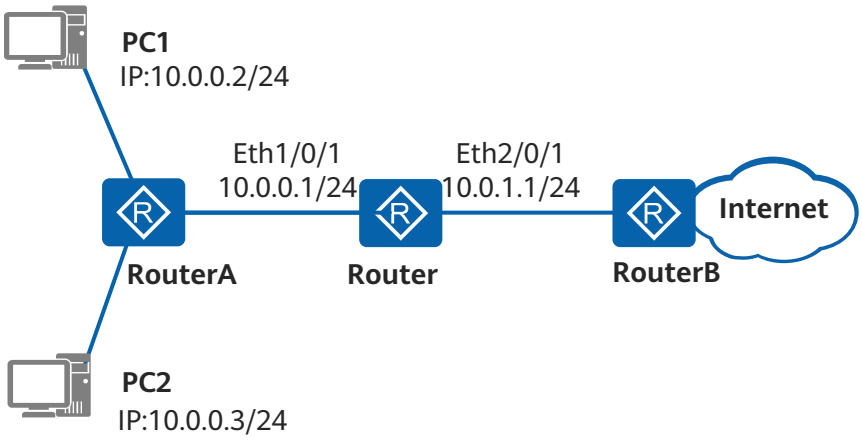
## Networking Requirements

In **Figure 5-16**, Eth1/0/1 of the Router is connected to PC1 and PC2, and Eth2/0/1 is connected to the upstream router. To prevent source address spoofing attacks,

 Copyright © Huawei Technologies Co., Ltd. 

the administrator configures URPF in strict mode on Eth1/0/1 and Eth2/0/1. In addition, the administrator expects the Router to perform URPF checks only on the packets from PC2 (10.0.0.3).

**Figure 5-16** Using basic ACLs to exclude valid packets from URPF check




## Configuration Roadmap

The following configurations are performed on the Router. The configuration roadmap is as follows:

1. Configure ACL-based URPF on Eth1/0/1 to perform URPF check only on the packets from PC2.
2. Configure URPF check mode on Eth2/0/1 to prevent source address spoofing attacks.

## Procedure

**Step 1** Configure ACL-based URPF on Eth1/0/1 to perform URPF check only on the packets from PC2.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface ethernet 1/0/1
[Router-Ethernet1/0/1] ip address 10.0.0.1 24
[Router-Ethernet1/0/1] urpf strict acl 2001
[Router-Ethernet1/0/1] quit
[Router] acl number 2001
[Router-acl-basic-2001] rule permit source 10.0.0.3 0.0.0.255
[Router-acl-basic-2001] quit
```

**Step 2** Configure URPF check on Eth2/0/1.

```
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] ip address 10.0.1.1 24
[Router-Ethernet2/0/1] urpf strict
[Router-Ethernet2/0/1] quit
```

**Step 3** Verify the configuration.

# Check the configuration of ACL rules.

```
[Router] display acl 2001
Basic ACL 2001, 1 rule
```

 Copyright © Huawei Technologies Co., Ltd. 

```
Acl's step is 5
 rule 5 permit source 10.0.0.0 0.0.0.255
```

# Check URPF configuration on Eth1/0/1.

```
[Router] interface ethernet 1/0/1
[Router-Ethernet1/0/1] display this
#
interface Ethernet1/0/1
 ip address 10.0.0.1 255.255.255.0
 urpf strict acl 2001
#
return
```

# Check URPF configuration on Eth2/0/1.

```
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] display this
#
interface Ethernet2/0/1
 ip address 10.0.1.1 255.255.255.0
 urpf strict
#
return
```

**----End**

## Configuration Files

Router configuration file

```
#
 sysname Router
#
acl number 2001
 rule 5 permit source 10.0.0.0 0.0.0.255
#
interface Ethernet1/0/1
 ip address 10.0.0.1 255.255.255.0
 urpf strict acl 2001
#
interface Ethernet2/0/1
 ip address 10.0.1.1 255.255.255.0
 urpf strict
#
return
```

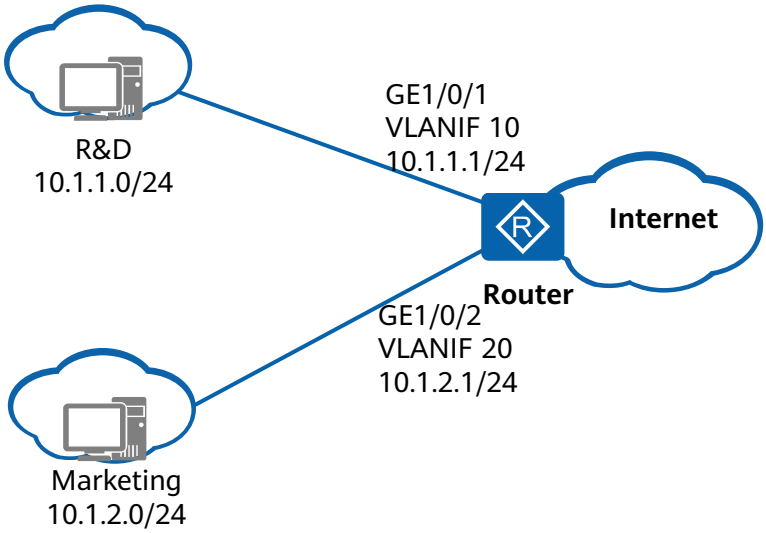
# 5.9.6 Example for Using Advanced ACLs to Restrict Mutual Access Between Network Segments

## Networking Requirements

As shown in **Figure 5-17**, the departments of an enterprise are connected through the Router. To facilitate network management, the administrator allocates the IP addresses on two network segments to the R&D and marketing departments respectively. In addition, the administrator adds the two departments to different VLANs for broadcast domain isolation. The Router needs to restrict mutual access between two network segments to ensure information security.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 5-17** Using advanced ACLs to restrict mutual access between network segments




## Configuration Roadmap

The following configurations are performed on the Router. The configuration roadmap is as follows:

1. Configure an advanced ACL and ACL-based traffic classifier to filter the packets exchanged between R&D and marketing departments.
2. Configure a traffic behavior to discard the packets matching the ACL rules.
3. Configure and apply a traffic policy to make the ACL and traffic behavior take effect.

## Procedure

**Step 1** Configure VLANs and IP addresses for interfaces to ensure network connections.

# Create VLAN 10 and VLAN 20.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10 20
```

# Configure GE1/0/1 and GE1/0/2 on the Router as trunk interfaces and add the interfaces to VLAN 10 and VLAN 20 respectively.

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] port link-type trunk
[Router-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[Router-GigabitEthernet1/0/1] quit
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] port link-type trunk
[Router-GigabitEthernet1/0/2] port trunk allow-pass vlan 20
[Router-GigabitEthernet1/0/2] quit
```

# Create VLANIF 10 and VLANIF 20 and assign IP addresses to them.

```
[Router] interface vlanif 10
[Router-Vlanif10] ip address 10.1.1.1 24
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router-Vlanif10] quit
[Router] interface vlanif 20
[Router-Vlanif20] ip address 10.1.2.1 24
[Router-Vlanif20] quit
```

**Step 2** Configure the ACL.

# Create advanced ACL 3001 and configure rules for the ACL to block the packets from the R&D department to the marketing department.

```
[Router] acl 3001
[Router-acl-adv-3001] rule deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[Router-acl-adv-3001] quit
```

# Create advanced ACL 3002 and configure rules for the ACL to block the packets from the marketing department to the R&D department.

```
[Router] acl 3002
[Router-acl-adv-3002] rule deny ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[Router-acl-adv-3002] quit
```

**Step 3** Configure an advanced ACL-based traffic classifier.

# Configure the traffic classifier **tc1** to classify packets that match ACL 3001 and ACL 3002.

```
[Router] traffic classifier tc1
[Router-classifier-tc1] if-match acl 3001
[Router-classifier-tc1] if-match acl 3002
[Router-classifier-tc1] quit
```

**Step 4** Configure a traffic behavior.

# Configure the traffic behavior **tb1** to reject packets.

```
[Router] traffic behavior tb1
[Router-behavior-tb1] deny
[Router-behavior-tb1] quit
```

**Step 5** Configure a traffic policy.

# Define the traffic policy and associate the traffic classifier and traffic behavior with the traffic policy.

```
[Router] traffic policy tp1
[Router-trafficpolicy-tp1] classifier tc1 behavior tb1
[Router-trafficpolicy-tp1] quit
```

**Step 6** Apply the traffic policy to interfaces.

# Packets from the R&D department are received by GE1/0/1 and packets from the marketing department are received by GE1/0/2; therefore, apply the traffic policy to the inbound direction of GE1/0/1 and GE1/0/2.

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] traffic-policy tp1 inbound
[Router-GigabitEthernet1/0/1] quit
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] traffic-policy tp1 inbound
[Router-GigabitEthernet1/0/2] quit
```

**Step 7** Verify the configuration.

# Check the configuration of ACL rules.

```
[Router] display acl 3001
Advanced ACL 3001, 1 rule
```

 Copyright © Huawei Technologies Co., Ltd. 

```
Acl's step is 5
 rule 5 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[Router] display acl 3002
Advanced ACL 3002, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
```

# Check the configuration of the traffic classifier.

```
[Router] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: class1
    Operator: OR
    Rule(s) :  -none-
   Classifier: tc1
    Operator: OR
    Rule(s) :
     if-match acl 3001
     if-match acl 3002
```

# Check the configuration of the traffic policy.

```
[Router] display traffic policy user-defined tp1
  User Defined Traffic Policy Information:
  Policy: tp1
   Classifier: tc1
    Operator: OR
     Behavior: tb1
      Deny
```

# The two network segments where the R&D and marketing departments reside cannot access each other.

**----End**

## Configuration Files

Router configuration file

```
#
 sysname Router
#
vlan batch 10 20
#
acl number 3001
 rule 5 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
acl number 3002
 rule 5 deny ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
traffic classifier tc1 operator or
 if-match acl 3001
 if-match acl 3002
#
traffic behavior tb1
 deny
#
traffic policy tp1
 classifier tc1 behavior tb1
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
```

 Copyright © Huawei Technologies Co., Ltd. 

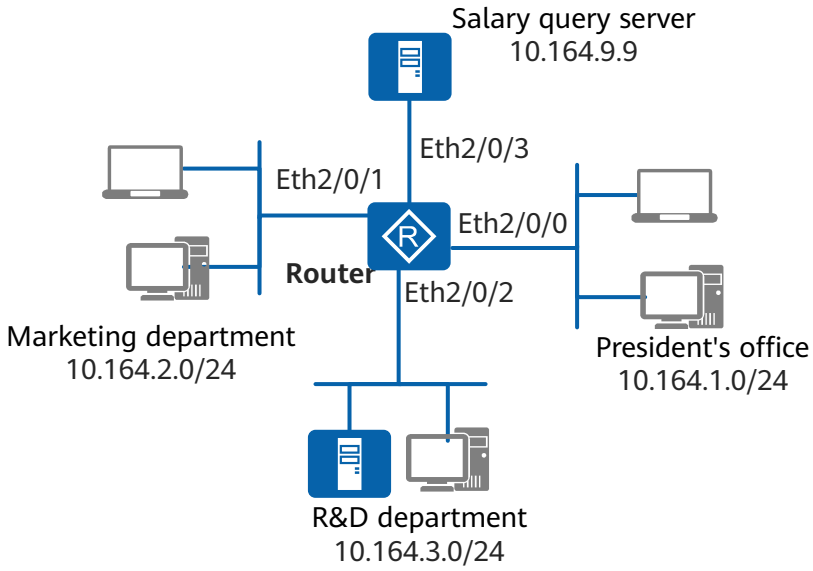
```
 port trunk allow-pass vlan 10
 traffic-policy tp1 inbound
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy tp1 inbound
#
return
```

# 5.9.7 Example for Using Advanced ACLs to Control Access to the Specified Server in the Specified Time Range

## Networking Requirements

As shown in **Figure 5-18**, the departments of an enterprise are connected through the Router. The R&D and marketing departments cannot access the salary query server at 10.164.9.9 in work hours (08:00 to 17:30), whereas the president office can access the server at anytime.

**Figure 5-18** Using advanced ACLs to control access to the specified server in the specified time range




## Configuration Roadmap

The following configurations are performed on the Router. The configuration roadmap is as follows:

1. Configure the time range, advanced ACL, and ACL-based traffic classifier to filter packets from users to the server in the specified time range. In this way, you can restrict the access of different users to the server in the specified time range.
2. Configure a traffic behavior to discard the packets matching the ACL.
3. Configure and apply a traffic policy to make the ACL and traffic behavior take effect.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Add interfaces to VLANs and assign IP addresses to the VLANIF interfaces.

# Add Eth2/0/0 - Eth2/0/2 to VLANs 10, 20, and 30 respectively, add Eth2/0/3 to VLAN 100, and assign IP addresses to the VLANIF interfaces. The configurations on Eth2/0/0 and VLANIF 10 are used as an example here. The configurations on Eth2/0/1, Eth2/0/2, and Eth2/0/3 are similar to those on Eth2/0/0, and the configurations on VLANIF 20, VLANIF 30, and VLANIF 100 are similar to the configurations on VLANIF 10.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10 20 30 100
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type trunk
[Router-Ethernet2/0/0] port trunk allow-pass vlan 10
[Router-Ethernet2/0/0] quit
[Router] interface vlanif 10
[Router-Vlanif10] ip address 10.164.1.1 255.255.255.0
[Router-Vlanif10] quit
```

**Step 2** Configure a time range.

# Configure the time range from 08:00 to 17:30.

```
[Router] time-range satime 8:00 to 17:30 working-day
```

**Step 3** Configure ACLs.

# Configure an ACL for the marketing department to access the salary query server.

```
[Router] acl 3002
[Router-acl-3002] rule deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0.0.0.0 time-range satime
[Router-acl-3002] quit
```

# Configure an ACL for the R&D department to access the salary query server.

```
[Router] acl 3003
[Router-acl-3003] rule deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0.0.0.0 time-range satime
[Router-acl-3003] quit
```

**Step 4** Configure ACL-based traffic classifiers.

# Configure the traffic classifier **c_market** to classify the packets that match ACL 3002.

```
[Router] traffic classifier c_market
[Router-classifier-c_market] if-match acl 3002
[Router-classifier-c_market] quit
```

# Configure the traffic classifier **c_rd** to classify the packets that match ACL 3003.

```
[Router] traffic classifier c_rd
[Router-classifier-c_rd] if-match acl 3003
[Router-classifier-c_rd] quit
```

**Step 5** Configure traffic behaviors.

# Configure the traffic behavior **b_market** to reject packets.

```
[Router] traffic behavior b_market
[Router-behavior-b_market] deny
[Router-behavior-b_market] quit
```

 Copyright © Huawei Technologies Co., Ltd. 

# Configure the traffic behavior **b_rd** to reject packets.

```
[Router] traffic behavior b_rd
[Router-behavior-b_rd] deny
[Router-behavior-b_rd] quit
```

**Step 6** Configure traffic policies.

# Configure the traffic policy **p_market** and associate the traffic classifier **c_market** and the traffic behavior **b_market** with the traffic policy.

```
[Router] traffic policy p_market
[Router-trafficpolicy-p_market] classifier c_market behavior b_market
[Router-trafficpolicy-p_market] quit
```

# Configure the traffic policy **p_rd** and associate the traffic classifier **c_rd** and the traffic behavior **b_rd** with the traffic policy.

```
[Router] traffic policy p_rd
[Router-trafficpolicy-p_rd] classifier c_rd behavior b_rd
[Router-trafficpolicy-p_rd] quit
```

**Step 7** Apply the traffic policy.

# Packets from the marketing department are received by Eth2/0/1, so apply the traffic policy **p_market** to the inbound direction of Eth2/0/1.

```
[Router] interface ethernet2/0/1
[Router-Ethernet2/0/1] traffic-policy p_market inbound
[Router-Ethernet2/0/1] quit
```

# Packets from the R&D department are received by Eth2/0/2, so apply the traffic policy **p_rd** to the inbound direction of Eth2/0/2.

```
[Router] interface ethernet2/0/2
[Router-Ethernet2/0/2] traffic-policy p_rd inbound
[Router-Ethernet2/0/2] quit
```

**Step 8** Verify the configuration.

# Check the configuration of ACL rules.

```
[Router] display acl all
 Total quantity of nonempty ACL number is 2

Advanced ACL 3002, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0 time-range satime(Active)

Advanced ACL 3003, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0 time-range satime(Active)
```

# Check the configuration of traffic classifiers.

```
[Router] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c_market
    Operator: OR
    Rule(s) :
     if-match acl 3002
   Classifier: c_rd
    Operator: OR
    Rule(s) :
     if-match acl 3003
```

# Check the configuration of traffic policies.

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router] display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: p_market
   Classifier: c_market
    Operator: OR
     Behavior: b_market
      Deny

  Policy: p_rd
   Classifier: c_rd
    Operator: OR
     Behavior: b_rd
      Deny
```

# Check the traffic policy use records.

```
[Router] display traffic-policy applied-record
----------------------------------------------------
  Policy Name:   p_market
  Policy Index:  6
     Classifier:c_market     Behavior:b_market
----------------------------------------------------
 *interface Ethernet2/0/1
    traffic-policy p_market inbound
      slot 0    :  success
----------------------------------------------------
  Policy Name:   p_rd
  Policy Index:  7
     Classifier:c_rd     Behavior:b_rd
----------------------------------------------------
 *interface Ethernet2/0/2
    traffic-policy p_rd inbound
      slot 0    :  success
----------------------------------------------------
```

# The R&D and marketing departments cannot access the salary query server in work hours (08:00 to 17:30).

**----End**

## Configuration Files

Router configuration file

```
#
 sysname Router
#
 time-range satime 08:00 to 17:30 working-day
#
vlan batch 10 20 30 100
#
acl number 3002
 rule 5 deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0 time-range
satime
acl number 3003
 rule 5 deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0 time-range satime
#
traffic classifier c_market operator or
 if-match acl 3002
traffic classifier c_rd operator or
 if-match acl 3003
#
traffic behavior b_market
 deny
traffic behavior b_rd
 deny
```

 Copyright © Huawei Technologies Co., Ltd. 

```
#
traffic policy p_market
 classifier c_market behavior b_market
traffic policy p_rd
 classifier c_rd behavior b_rd
#
interface Vlanif10
 ip address 10.164.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.164.2.1 255.255.255.0
#
interface Vlanif30
 ip address 10.164.3.1 255.255.255.0
#
interface Vlanif100
 ip address 10.164.9.9 255.255.255.0
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy p_market inbound
#
interface Ethernet2/0/2
 port link-type trunk
 port trunk allow-pass vlan 30
 traffic-policy p_rd inbound
#
interface Ethernet2/0/3
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

# 5.9.8 Example for Using an Advanced ACL to Configure the Firewall Function

## Networking Requirements

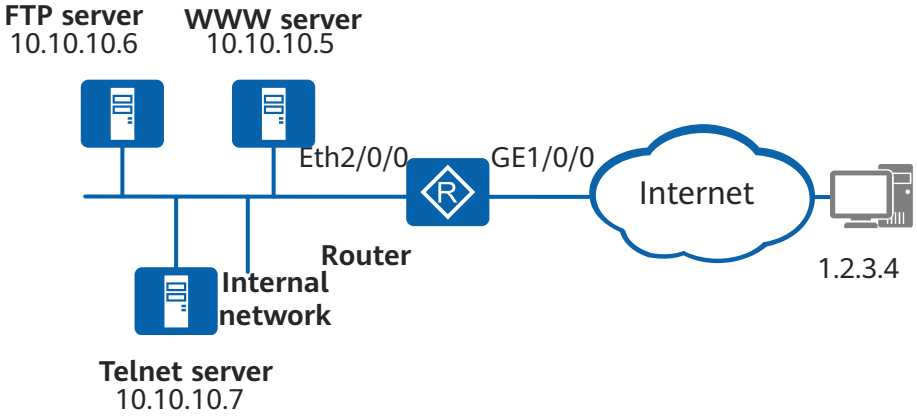
As shown in **Figure 5-19**, an enterprise network running the Web, FTP, and Telnet services accesses an external network through GE1/0/0 and joins a VLAN through Eth2/0/0.

The enterprise network segment is 10.10.10.0/24 and the IP addresses of the Web server, FTP server, and Telnet server are 10.10.10.5/24, 10.10.10.6/24, and 10.10.10.7/24.

To ensure security, the Router provides the firewall function. Only specified users are allowed to access internal servers of the enterprise and only internal servers of the enterprise are allowed to access the external network.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 5-19** Using advanced an ACL to configure the firewall function




## Configuration Roadmap

The following configurations are performed on the Router. The configuration roadmap is as follows:

1. Configure zones on the internal and external networks.
2. Configure an interzone and enable the firewall function in the interzone.
3. Configure advanced ACLs to restrict the rights to access the internal servers and external network.
4. Configure ACL-based packet filtering in the interzone.

## Procedure

**Step 1** Configure zones.

# Configure a zone on the internal network.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] firewall zone company
[Router-zone-company] priority 12
[Router-zone-company] quit
```

# Add interfaces to VLANs and assign IP addresses to the VLANIF interfaces. Add VLANIF 100 to the zone **company**.

```
[Router] vlan batch 100
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type access
[Router-Ethernet2/0/0] port default vlan 100
[Router-Ethernet2/0/0] quit
[Router] interface vlanif 100
[Router-Vlanif100] ip address 10.10.10.1 255.255.255.0
[Router-Vlanif100] zone company
[Router-Vlanif100] quit
```

# Configure a zone on the external network.

```
[Router] firewall zone external
[Router-zone-external] priority 5
[Router-zone-external] quit
```

 Copyright © Huawei Technologies Co., Ltd. 

# Add GigabitEthernet 1/0/0 to the zone **external**.

```
[Router] interface gigabitethernet 1/0/0
[Router-gigabitethernet1/0/0] ip address 10.39.10.8 255.255.255.0
[Router-gigabitethernet1/0/0] zone external
[Router-gigabitethernet1/0/0] quit
```

**Step 2** Configure an interzone.

```
[Router] firewall interzone company external
[Router-interzone-company-external] firewall enable
[Router-interzone-company-external] quit
```

**Step 3** Configure ACL 3001.

# Create ACL 3001.

```
[Router] acl 3001
```

# Configure a rule in ACL 3001 to allow specified users to access internal servers.

```
[Router-acl-adv-3001] rule permit tcp source 1.2.3.4 0.0.0.0 destination 10.10.10.5 0.0.0.0
[Router-acl-adv-3001] rule permit tcp source 1.2.3.4 0.0.0.0 destination 10.10.10.6 0.0.0.0
[Router-acl-adv-3001] rule permit tcp source 1.2.3.4 0.0.0.0 destination 10.10.10.7 0.0.0.0
```

# Configure a rule in ACL 3001 to prevent other users from accessing any host of the enterprise.

```
[Router-acl-adv-3001] rule deny ip
[Router-acl-adv-3001] quit
```

**Step 4** Configure ACL 3002.

# Create ACL 3002.

```
[Router] acl 3002
```

# Configure a rule in ACL 3002 to allow internal servers to access the external network.

```
[Router-acl-adv-3002] rule permit ip source 10.10.10.5 0.0.0.0
[Router-acl-adv-3002] rule permit ip source 10.10.10.6 0.0.0.0
[Router-acl-adv-3002] rule permit ip source 10.10.10.7 0.0.0.0
```

# Configure a rule in ACL 3002 to prevent other users of the enterprise from accessing the external network.

```
[Router-acl-adv-3002] rule deny ip
[Router-acl-adv-3002] quit
```

**Step 5** Configure ACL-based packet filtering in the interzone.

```
[Router] firewall interzone company external
[Router-interzone-company-external] packet-filter 3001 inbound
[Router-interzone-company-external] packet-filter 3002 outbound
[Router-interzone-company-external] quit
```

**Step 6** Verify the configuration.

# After the configuration is complete, only the host at 1.2.3.4 can access internal servers and only internal servers can access the external network.

# Run the **display firewall interzone** [ *zone-name1 zone-name2* ] command on the Router. The result is as follows:

```
[Router] display firewall interzone company external
interzone company external
 firewall enable
 packet-filter default deny inbound
```

```
 packet-filter default permit outbound
 packet-filter 3001 inbound
 packet-filter 3002 outbound
```

**----End**

## Configuration Files

Configuration file of the Router

```
#
 sysname Router
#
 vlan batch 100
#
acl number 3001
 rule 5 permit tcp source 1.2.3.4 0 destination 10.10.10.5 0
 rule 10 permit tcp source 1.2.3.4 0 destination 10.10.10.6 0
 rule 15 permit tcp source 1.2.3.4 0 destination 10.10.10.7 0
 rule 20 deny ip
acl number 3002
 rule 5 permit ip source 10.10.10.5 0
 rule 10 permit ip source 10.10.10.6 0
 rule 15 permit ip source 10.10.10.7 0
 rule 20 deny ip
#
interface Vlanif100
 ip address 10.10.10.1 255.255.255.0
 zone company
#
firewall zone company
 priority 12
#
firewall zone external
 priority 5
#
firewall interzone company external
 firewall enable
 packet-filter 3001 inbound
 packet-filter 3002 outbound
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 100
#
interface GigabitEthernet1/0/0
 ip address 10.39.10.8 255.255.255.0
 zone external
#
return
```

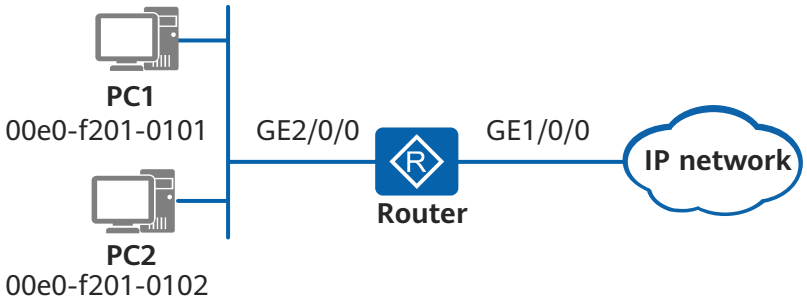
# 5.9.9 Example for Using Layer 2 ACLs to Block Network Access of the Specified Users

## Networking Requirements

As shown in **Figure 5-20**, the Router that functions as the gateway is connected to the users' PCs. The administrator wants to block network access of PC1 after detecting that PC1 (00e0-f201-0101) is an unauthorized user.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 5-20** Using Layer 2 ACLs to block network access of the specified users




## Configuration Roadmap

The following configurations are performed on the Router. The configuration roadmap is as follows:

1. Configure a Layer 2 ACL and ACL-based traffic classifier to discard packets from MAC address 00e0-f201-0101 (preventing the user with this MAC address from accessing the network).
2. Configure a traffic behavior to discard the packets matching the ACL.
3. Configure and apply a traffic policy to make the ACL and traffic behavior take effect.

## Procedure

**Step 1** Configure an ACL.

# Configure a Layer 2 ACL to meet the preceding requirement.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] acl 4000
[Router-acl-L2-4000] rule deny source-mac 00e0-f201-0101 ffff-ffff-ffff
[Router-acl-L2-4000] quit
```

**Step 2** Configure an ACL-based traffic classifier.

# Configure the traffic classifier **tc1** to classify packets that match ACL 4000.

```
[Router] traffic classifier tc1
[Router-classifier-tc1] if-match acl 4000
[Router-classifier-tc1] quit
```

**Step 3** Configure a traffic behavior.

# Configure the traffic behavior **tb1** to reject packets.

```
[Router] traffic behavior tb1
[Router-behavior-tb1] deny
[Router-behavior-tb1] quit
```

**Step 4** Configure a traffic policy.

# Configure the traffic policy **tp1** and associate **tc1** and **tb1** with the traffic policy.

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router] traffic policy tp1
[Router-trafficpolicy-tp1] classifier tc1 behavior tb1
[Router-trafficpolicy-tp1] quit
```

**Step 5** Apply the traffic policy.

# Packets from PC1 to the Internet are received by GE2/0/0, so apply the traffic policy **tp1** to the inbound direction of GE2/0/0.

```
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] traffic-policy tp1 inbound
[Router-GigabitEthernet2/0/0] quit
```

**Step 6** Verify the configuration.

# Check the configuration of the ACL rule.

```
[Router] display acl 4000
L2 ACL 4000, 1 rule
Acl's step is 5
 rule 5 deny source-mac 00e0-f201-0101
```

# Check the configuration of the traffic classifier.

```
[Router] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: tc1
    Operator: OR
    Rule(s) :
     if-match acl 4000
```

# Check the configuration of the traffic policy.

```
[Router] display traffic policy user-defined tp1
  User Defined Traffic Policy Information:
  Policy: tp1
   Classifier: tc1
    Operator: OR
     Behavior: tb1
      Deny
```

# The user with MAC address 00e0-f201-0101 cannot access the Internet.

**----End**

## Configuration Files

Router configuration file

```
#
 sysname Router
#
acl number 4000
 rule 5 deny source-mac 00e0-f201-0101
#
traffic classifier tc1 operator or
 if-match acl 4000
#
traffic behavior tb1
 deny
#
traffic policy tp1
 classifier tc1 behavior tb1
#
interface GigabitEthernet2/0/0
 traffic-policy tp1 inbound
#
return
```

 Copyright © Huawei Technologies Co., Ltd. 

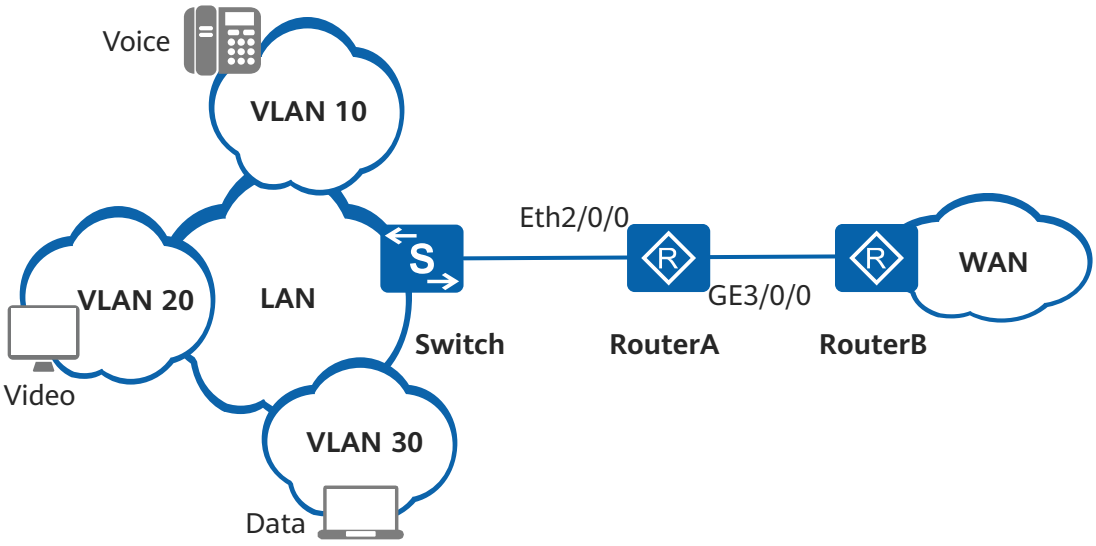
# 5.9.10 Example for Using Layer 2 ACLs in QoS to Implement Traffic Policing

## Networking Requirements

As shown in **Figure 5-21**, voice, video, and data services on the LAN of the enterprise belong to VLAN10, VLAN20, and VLAN30 respectively. The services are transmitted to Eth2/0/0 of RouterA through the switch, and are then transmitted to the WAN through GE3/0/0 of RouterA.

Flow-based traffic policing needs to be performed for different service packets on RouterA to limit the rate of each service flow within a proper range, so that bandwidth can be ensured for each service. Interface-based traffic policing needs to be performed for all incoming traffic on Eth2/0/0 so that the total traffic rate of the enterprise is limited within a proper range.

**Figure 5-21** Networking diagram of traffic policing




## Configuration Roadmap

The following configurations are performed on the Router. The configuration roadmap is as follows:

1. Create VLANs and VLANIF interfaces on RouterA and configure physical interfaces to ensure that enterprise users can access the WAN through RouterA.
2. Configure traffic classifiers on RouterA to classify packets based on VLAN IDs.
3. Configure traffic behaviors on RouterA to perform traffic policing for different service flows from the enterprise.


Copyright © Huawei Technologies Co., Ltd.

4. Configure a traffic policy on RouterA, associate the traffic behaviors with traffic classifiers in the traffic policy, and apply the traffic policy to the inbound direction of the interface on RouterA connected to the switch.
5. Configure interface-based traffic policing in the inbound direction of the interface on RouterA connected to the switch to limit the rate of all the packets.

## Procedure

**Step 1** Configure VLANs and interfaces.

# Create VLAN10, VLAN20, and VLAN30 on RouterA.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan batch 10 20 30
```

# Configure Eth2/0/0 as a trunk interface and allow packets from VLAN10, VLAN20, and VLAN30 to pass through.

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] port link-type trunk
[RouterA-Ethernet2/0/0] port trunk allow-pass vlan 10 20 30
[RouterA-Ethernet2/0/0] quit
```

NOTE

Configure the interface on the switch connected to RouterA as a trunk interface and allow packets from VLAN 10, VLAN 20, and VLAN 30 to pass through.

# Create VLANIF10, VLANIF20, and VLANIF30, and assign IP addresses 192.168.1.1/24, 192.168.2.1/24, and 192.168.3.1/24 to VLANIF 10, VLANIF20, and VLANIF30 respectively.

```
[RouterA] interface vlanif 10
[RouterA-Vlanif10] ip address 192.168.1.1 24
[RouterA-Vlanif10] quit
[RouterA] interface vlanif 20
[RouterA-Vlanif20] ip address 192.168.2.1 24
[RouterA-Vlanif20] quit
[RouterA] interface vlanif 30
[RouterA-Vlanif30] ip address 192.168.3.1 24
[RouterA-Vlanif30] quit
```

# Set the IP address of GE3/0/0 to 192.168.4.1/24.

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.4.1 24
[RouterA-GigabitEthernet3/0/0] quit
```

# Configure RouterB and ensure that there are reachable routes between RouterB and RouterA.

**Step 2** Configure traffic classifiers.

# Configure traffic classifiers **c1**, **c2**, and **c3** on RouterA to match different service flows from the enterprise based on VLAN IDs.

```
[RouterA] traffic classifier c1
[RouterA-classifier-c1] if-match vlan-id 10
[RouterA-classifier-c1] quit
[RouterA] traffic classifier c2
[RouterA-classifier-c2] if-match vlan-id 20
[RouterA-classifier-c2] quit
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[RouterA] traffic classifier c3
[RouterA-classifier-c3] if-match vlan-id 30
[RouterA-classifier-c3] quit
```

**Step 3** Configure traffic behaviors.

# Create traffic behaviors **b1**, **b2**, and **b3** on RouterA to perform traffic policing for different service flows from the enterprise.

```
[RouterA] traffic behavior b1
[RouterA-behavior-b1] car cir 256
[RouterA-behavior-b1] statistic enable
[RouterA-behavior-b1] quit
[RouterA] traffic behavior b2
[RouterA-behavior-b2] car cir 4000
[RouterA-behavior-b2] statistic enable
[RouterA-behavior-b2] quit
[RouterA] traffic behavior b3
[RouterA-behavior-b3] car cir 2000
[RouterA-behavior-b3] statistic enable
[RouterA-behavior-b3] quit
```

**Step 4** Configure a traffic policy and apply the traffic policy to Eth2/0/0.

# Create a traffic policy **p1** on RouterA, associate the traffic behaviors with traffic classifiers in the traffic policy, and apply the traffic policy to Eth2/0/0 in the inbound direction.

```
[RouterA] traffic policy p1
[RouterA-trafficpolicy-p1] classifier c1 behavior b1
[RouterA-trafficpolicy-p1] classifier c2 behavior b2
[RouterA-trafficpolicy-p1] classifier c3 behavior b3
[RouterA-trafficpolicy-p1] quit
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] traffic-policy p1 inbound
```

**Step 5** Configure interface-based traffic policing.

# Configure interface-based traffic policing in the inbound direction of Eth2/0/0 on RouterA to limit the total traffic rate of the enterprise within a proper range.

```
[RouterA-Ethernet2/0/0] qos car inbound cir 10000
[RouterA-Ethernet2/0/0] quit
```

**Step 6** Verify the configuration.

# View the traffic classifier configuration.

```
[RouterA] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c2
    Operator: OR
    Rule(s) :
     if-match vlan-id 20
   Classifier: c3
    Operator: OR
    Rule(s) :
     if-match vlan-id 30
   Classifier: c1
    Operator: OR
    Rule(s) :
     if-match vlan-id 10
```

# View the traffic policy configuration.

```
[RouterA] display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: p1
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 Classifier: c1
  Operator: OR
   Behavior: b1
    Committed Access Rate:
      CIR 256 (Kbps), PIR 0 (Kbps), CBS 48128 (byte), PBS 80128 (byte)
      Color Mode: color Blind
      Conform Action: pass
      Yellow  Action: pass
      Exceed  Action: discard
    statistic: enable

 Classifier: c2
  Operator: OR
   Behavior: b2
    Committed Access Rate:
      CIR 4000 (Kbps), PIR 0 (Kbps), CBS 752000 (byte), PBS 1252000 (byte)
      Color Mode: color Blind
      Conform Action: pass
      Yellow  Action: pass
      Exceed  Action: discard
    statistic: enable

 Classifier: c3
  Operator: OR
   Behavior: b3
    Committed Access Rate:
      CIR 2000 (Kbps), PIR 0 (Kbps), CBS 376000 (byte), PBS 626000 (byte)
      Color Mode: color Blind
      Conform Action: pass
      Yellow  Action: pass
      Exceed  Action: discard
    statistic: enable
```

# View the traffic policy configuration on Eth2/0/0.

```
[RouterA] display traffic policy statistics interface ethernet 2/0/0 inbound

 Interface: Ethernet2/0/0
 Traffic policy inbound: p1
 Rule number: 3
 Current status: OK!
Item                  Sum(Packets/Bytes)            Rate(pps/bps)
-------------------------------------------------------------------------------
Matched                       0/0                       0/0
  Passed                     0/0                       0/0
  Dropped                     0/0                       0/0
    Filter                   0/0                       0/0
    CAR                      0/0                       0/0
  Queue Matched                0/0                       0/0
    Enqueued                  0/0                       0/0
    Discarded                 0/0                       0/0
  CAR                        0/0                       0/0
    Green packets              0/0                       0/0
    Yellow packets             0/0                       0/0
    Red packets                0/0                       0/0
```

**----End**

## Configuration Files

- RouterA configuration file

```
#
 sysname RouterA
#
vlan batch 10 20 30
#
traffic classifier c1 operator or
 if-match vlan-id 10
```

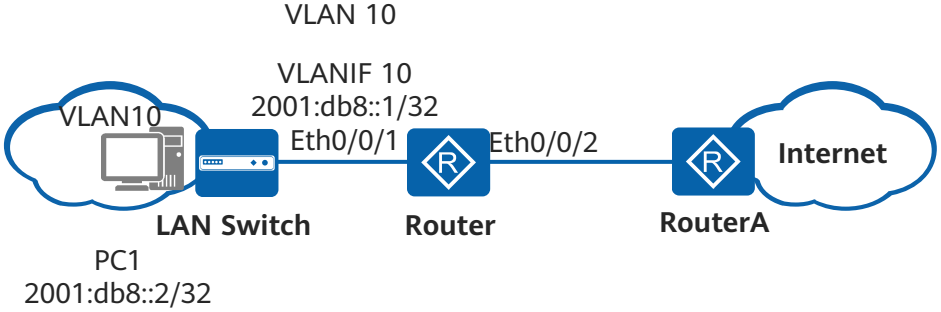
```
traffic classifier c2 operator or
 if-match vlan-id 20
traffic classifier c3 operator or
 if-match vlan-id 30
#
traffic behavior b1
 car cir 256 cbs 48128 pbs 80128 green pass yellow pass red discard
 statistic enable
traffic behavior b2
 car cir 4000 cbs 752000 pbs 1252000 green pass yellow pass red discard
 statistic enable
traffic behavior b3
 car cir 2000 cbs 376000 pbs 626000 green pass yellow pass red discard
 statistic enable
#
traffic policy p1
 classifier c1 behavior b1
 classifier c2 behavior b2
 classifier c3 behavior b3
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
 ip address 192.168.3.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 10 20 30
 qos car inbound cir 10000
 traffic-policy p1 inbound
#
interface GigabitEthernet3/0/0
 ip address 192.168.4.1 255.255.255.0
#
return
```

# 5.9.11 Example for Using Advanced ACL6s to Filter Certain Types of IPv6 Packets

## Networking Requirements

As shown in **Figure 5-22**, users are connected to the Router through Eth0/0/1. The Router needs to block the certain types of IPv6 packets from users in which the source IPv6 address is host address 2001:db8::2/32 and destination IPv6 address is 2001:db8::1/32.

**Figure 5-22** Using advanced ACL6s to filter certain types of IPv6 packets




 Copyright © Huawei Technologies Co., Ltd. 

## Configuration Roadmap

The following configurations are performed on the Router. The configuration roadmap is as follows:

1. Configure an advanced ACL6 and ACL6-based traffic classifier to filter the IPv6 packets in which the source IPv6 address is host address 2001:db8::2/32 and destination IPv6 address is 2001:db8::2/32.
2. Configure a traffic behavior to discard the packets matching the ACL6.
3. Configure and apply a traffic policy to make the ACL6 and traffic behavior take effect.

## Procedure

**Step 1** Enable the IPv6 forwarding capability, add an interface to a VLAN, and assign an IPv6 address to the VLANIF interface.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] ipv6
[Router] vlan batch 10
[Router] interface ethernet 0/0/1
[Router-Ethernet0/0/1] port link-type trunk
[Router-Ethernet0/0/1] port trunk allow-pass vlan 10
[Router-Ethernet0/0/1] quit
[Router] interface vlanif 10
[Router-Vlanif10] ipv6 enable
[Router-Vlanif10] ipv6 address 2001:db8::1 32
[Router-Vlanif10] quit
```

**Step 2** Configure an advanced ACL6 and ACL6-based traffic classifier. Configure a traffic behavior and traffic policy, and apply the traffic policy to the inbound direction of Eth0/0/1 to reject the IPv6 packets with source IPv6 address 2001:db8::2/32 and destination IPv6 address 2001:db8::1/32.

```
[Router] acl ipv6 number 3001
[Router-acl6-adv-3001] rule deny ipv6 source 2001:db8::2/32 destination 2001:db8::1/32
[Router-acl6-adv-3001] quit
[Router] traffic classifier class1
[Router-classifier-class1] if-match ipv6 acl 3001
[Router-classifier-class1] quit
[Router] traffic behavior behav1
[Router-behavior-behav1] deny
[Router-behavior-behav1] quit
[Router] traffic policy policy1
[Router-trafficpolicy-policy1] classifier class1 behavior behav1
[Router-trafficpolicy-policy1] quit
[Router] interface ethernet 0/0/1
[Router-Ethernet0/0/1] traffic-policy policy1 inbound
[Router-Ethernet0/0/1] quit
```

**Step 3** Verify the configuration.

# Check the ACL6 configuration.

```
[Router] display acl ipv6 3001

Advanced IPv6 ACL 3001, 1 rule
Acl's step is 5
 rule 5 deny ipv6 source 2001:db8::2/32 destination 2001:db8::1/32
```

# Check the configuration of the traffic classifier.

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: class1
    Operator: OR
    Rule(s) :
     if-match ipv6 acl 3001
```

# Check the configuration of the traffic policy.

```
[Router] display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: policy1
    Classifier: class1
      Operator: OR
       Behavior: behav1
        Deny
```

**----End**

## Configuration Files

Router configuration file

```
#
 sysname Router
#
acl ipv6 number 3001
 rule 5 deny ipv6 source 2001:db8::2/32 destination 2001:db8::1/32
#
ipv6
#
vlan batch 10
#
traffic classifier class1 operator or
 if-match ipv6 acl 3001
#
traffic behavior behav1
 deny
#
traffic policy policy1
 classifier class1 behavior behav1
#
interface Vlanif10
 ipv6 enable
 ipv6 address 2001:db8::1/32
#
interface Ethernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 traffic-policy policy1 inbound
#
return
```

# 5.10 Troubleshooting ACLs

## 5.10.1 Services Are Interrupted Due to Incorrect IP Address Wildcard Mask

### Fault Description

A traffic policy has been configured on a device to redirect packets. To redirect the packets from a certain IP address, the administrator adds a rule to the ACL used

 Copyright © Huawei Technologies Co., Ltd. 

by the traffic policy following the ACL configuration principle. The new rule uses this source IP address as the matching condition. However, the IP address wildcard mask in the rule is incorrectly configured. As a result, BGP packets cannot be sent to the CPU and most services are interrupted.

## Procedure

**Step 1** Run the **display this** command in the ACL view to check the new rule.

The new rule is as follows:

```
rule 100 permit ip source 10.1.1.3 255.255.255.255
```

The IP address wildcard mask is 255.255.255.255, which is not an inverse mask. This rule is equivalent to "rule 100 permit ip" and "rule 100 permit ip source any", meaning that packets from any IP address are matched.

The traffic policy using this ACL has been applied to a large number of interfaces, so all BGP packets received by these interfaces are redirected to other interfaces, but not sent to the CPU. The device times out to process protocol packets and most services are interrupted.

**Step 2** Run the **rule (advanced ACL view)** command in the ACL view to modify the IP address wildcard mask in the new rule.

The modified rule is as follows:

```
rule 100 permit ip source 10.1.1.3 0.0.0.0 //indicates the IP address of a single host only when the IP address wildcard mask is 0.0.0.0.
```

Services are recovered, and packets from source IP address 10.1.1.3 are redirected correctly.

**----End**

# 5.10.2 Users Cannot Access the Internet Because the DNS Server Address Is Blocked

## Fault Description

An ACL is configured on the device to restrict the destination addresses that can be accessed by users; however, the DNS server address is blocked in the ACL. As a result, the query packets sent from users to the DNS server are discarded. The domain names cannot be resolved, so users cannot access the Internet.

## Procedure

**Step 1** Run the **display acl** command in the system view to check ACL rules.

The following rule is included:

```
rule 100 deny ip destination 10.102.192.0 0.0.0.255  //Reject the packets from network segment 10.102.192.0/24.
```

The DNS server address configured on user PCs is 10.102.192.68, which belongs to network segment 10.102.192.0/24. Therefore, packets sent from users to the DNS

 Copyright © Huawei Technologies Co., Ltd. 

server are discarded. The domain names cannot be resolved, so users cannot access the Internet.

**Step 2** Run the **rule (advanced ACL view)** command in the ACL view to add a rule to permit the DNS server address.

```
rule 99 permit ip destination 10.102.192.68 0  //Permit the packets destined for the DNS server.
rule 100 deny ip destination 10.102.192.0 0.0.0.255  //Reject the packets destined for network segment 10.102.192.0/24.
```

After rule 99 is added, the packets sent from users to the DNS server match rule 99 and pass. The domain names can be resolved, and users can access the Internet.

**----End**

# 5.10.3 Time Range-based ACL Does Not Take Effect Due to Incorrect System Time

## Fault Description

The system time on the device is incorrect, so the time range-based ACL does not take effect.

## Procedure

**Step 1** Run the **display acl** command in the system view to check ACL rules.

A rule based on time range is included:

```
rule 10 deny ip source 10.1.1.1 0 time-range time1 //Reject the packets from 10.1.1.1 in the time range time1.
```

**Step 2** Run the **display time-range** { **all** | *time-name* } command in the system view to check the configuration of time range **time1**.

The following information is displayed:

```
Current time is 14:53:17 8-16-2013 Friday

Time-range: time1 ( Inactive )
from 00:00 2014/1/1 to 23:59 2014/12/31
Total time-range number is 1
```

The time range **time1** starts at 00:00 on January 1, 2014 and ends at 23:59 on December 31, 2014, while the system time is 14:53:17 on August 16, 2013. The actual date is August 16, 2014. The system time on the device is not within the time range **time1**. Therefore, the ACL associating with **time1** does not take effect, and packets from 10.1.1.1 are not discarded.

**Step 3** Change the system date and time.

- Correct the system date and time.

  Run the **clock datetime** command in the user view.

  ```
  clock datetime 14:53:17 2014-08-16 //Set the date to 2014-08-16.
  ```

- Configure NTP to enable automatic clock synchronization on the device so that the device can synchronize clock with a trusted device (which has been synchronized clock with an authoritative clock through network).

 Copyright © Huawei Technologies Co., Ltd. 

a. On the trusted device, configure the NTP master clock and clock stratum.

   Run the **ntp-service refclock-master** command in the system view.

   ```
   ntp-service refclock-master 2 //A small stratum value indicates a high precision.
   ```

b. On the device that needs to synchronize clock with the trusted device, set the NTP working mode. For details, see Configuring NTP Operating Modes.

**----End**

# 5.11 FAQ About ACLs

## 5.11.1 In Which Methods Can ACLs Be Delivered?

After an ACL is configured, it must be applied to a service module so that the ACL rules can be delivered and take effect.

Usually, an ACL is applied to a traffic policy or simplified traffic policy so that the device can deliver ACL rules globally, or on an interface to filter packets to be forwarded. In addition, an ACL can be applied to the service modules such as Telnet, FTP, and routing.

**Table 5-21** describes the common ACL delivery methods.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 5-21** ACL delivery methods

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Filtering packets to be forwarded | The device filters received packets globally, or on an interface, and then discards, modifies priorities of, or redirects the filtered packets.<br>For example, you can use ACL to reduce the service level for the bandwidth-consuming services, such as P2P downloading and online video. When network congestion occurs, these packets are discarded first. | • Simplified traffic policy: See ACL-based Simplified Traffic Policy Configuration in *Huawei AR Series Access Routers Configuration Guide - QoS*.<br>• Traffic policy: See MQC Configuration in *Huawei AR Series Access Routers Configuration Guide - QoS*.<br>• Packet filtering firewall: See **6.7 Configuring the Packet Filtering Firewall** in *Huawei AR Series Access Routers Configuration Guide - Firewall*.<br>• Dynamic NAT: See Configuring Dynamic NAT in the *Huawei AR Series Access Routers Configuration Guide - IP Services*.<br>• NAT server: See Configuring an Internal NAT Server in the *Huawei AR Series Access Routers Configuration Guide - IP Services*. |
| Filtering packets to be sent to the CPU | If too many protocol packets are sent to the CPU, the CPU usage increases and CPU performance degrades. The device restricts the packets to be sent to the CPU.<br>For example, when a user sends a large number of ARP attack packets to the device, the CPU is busy and service is interrupted. You can apply an ACL to the local attack defense service, and add the user to the blacklist so that the CPU discards the packets from this user. | Blacklist: See **8.4.2 Configuring a Blacklist** in Local Attack Defense Configuration. |

 Copyright © Huawei Technologies Co., Ltd. 

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Login control | The device controls access permission of users. Only authorized users can log in to the device, and other users cannot log in without permission. This ensures network security. | • Telnet: See Enabling the Telnet Server Function in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• FTP: See Managing Files When the Device Functions as an FTP Server in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• SFTP: See Managing Files When the Device Functions as an SFTP Server in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• TFTP: See Managing Files When the Device Functions as a TFTP Client in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• Web login: See (Optional) Configuring Web System Parameters in *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.<br>• SNMP: See (Optional) Restricting Management Rights of the NMS (SNMPv1 and SNMPv2c) and (Optional) Restricting Management Rights of the NMS (SNMPv3) in *Huawei AR Series Access Routers Configuration Guide - Network Management and Monitoring*. |

 Copyright © Huawei Technologies Co., Ltd. 

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| Route filtering | ACLs can be applied to various dynamic routing protocols to filter advertised and received routes and multicast groups.<br>For example, you can apply an ACL to a routing policy to prevent the device from sending routes of a network segment to the neighboring router. | • BGP: See Controlling the Advertisement of BGP Routes and Controlling the Receiving of BGP Routes in *Huawei AR Series Access Routers Configuration Guide - IP Unicast Routing*.<br>• IS-IS (IPv4): See Configuring IS-IS to Advertise Specified External Routes to an IS-IS Routing Domain and Adding Specified IS-IS Routes to the IP Routing Table in *Huawei AR Series Access Routers Configuration Guide - IP Unicast Routing*.<br>• OSPF: See Configuring OSPF to Filter the Received Routes, Configuring OSPF to Filter the Routes to Be Advertised, and (Optional) Configuring GR Session Parameters on the Helper in *Huawei AR Series Access Routers Configuration Guide - IP Unicast routing*.<br>• RIP: See Configuring RIP to Import Routes and Configuring RIP to Filter Received Routes in *Huawei AR Series Access Routers Configuration Guide - IP Unicast routing*.<br>• Multicast: See Filtering IGMP Messages Based on Source IP Addresses, Configuring a Multicast Group Policy, (Optional) Configuring the Range of Multicast Groups That an Interface Can Join, and (Optional) Configuring an SSM Group Policy in *Huawei AR Series Access* |

 Copyright © Huawei Technologies Co., Ltd. 

| Service Category | Usage Scenario | How ACLs Are Used |
| --- | --- | --- |
| | | *Routers Configuration Guide - IP Multicast*. |

## 5.11.2 What Is the Relationship Between the permit/deny Rules in an ACL and Those in the Behavior of a Traffic Policy?

An ACL is usually used with a traffic policy. A traffic policy includes the traffic classifier that meets the requirement of an ACL and a traffic behavior, such as permit/deny.

The permit/deny rules in an ACL and a behavior in the traffic policy are used as follows.

**Table 5-22** Usage of permit/deny rules in an ACL and in a behavior

| ACL | Behavior in a Traffic Policy | Action Taken for Matching Packets |
| --- | --- | --- |
| permit | permit | permit |
| permit | deny | deny |
| deny | permit | deny |
| deny | deny | deny |

NOTE

The traffic policy module permits packets by default. If you just want to block mutual access between network segments, you only need to define the characteristics of the packets to be denied in the ACL. If you add **rule permit** at the bottom of the ACL, the packets that do not match previous rules will match the last rule. In addition, if the traffic behavior is set to deny, the device discards all packets matching **rule permit**. As a result, all services are interrupted.

## 5.11.3 How Can I Check the Order in Which ACL Rules Take Effect?

Run the **display acl** { *acl-number* | **name** *acl-name* | **all** } or **display acl ipv6** { *acl6-number* | **name** *acl6-name* | **all** } command in any view or the **display this** command in the ACL view to check the order in which ACL rules take effect, as shown in **Table 5-23**.


Copyright © Huawei Technologies Co., Ltd.

**Table 5-23** ACL matching order

| ACL Type | Order |
| --- | --- |
| ACL in **config** mode | The rules with smaller IDs take effect earlier than the rules with larger IDs. |
| ACL in **auto** mode | The rules with smaller IDs take effect earlier than the rules with larger IDs. |
| ACL6 in **config** mode | The rules with smaller IDs take effect earlier than the rules with larger IDs. |
| ACL6 in **auto** mode | The rules in front lines take effect earlier than the rules in latter lines. The rules are arranged in the ascending order of rule IDs. |

NOTE

When multiple traffic policies using ACLs are applied to a device, if a packet matches the ACL rules in different traffic policies, the matching order of the ACL rules depends on the processing mechanism of the traffic policy module. For details, see *Huawei AR Series Access Routers Configuration Guide - QoS*.

## 5.11.4 How Can Unidirectional Access Control Be Implemented?

You can use one of the following methods to implement unidirectional access control.

NOTE

The following commands are only for you reference. You should comply with the command line syntax of the version running on your device.

- Method 1: Traffic policy
  a. Configure an advanced ACL.

     Run the **acl** [ **number** ] *acl-number* [ **match-order** { **auto** | **config** } ] command in the system view to create an advanced ACL (3000-3999) and enter the advanced ACL view or run the **acl name** *acl-name* { **advance** | *acl-number* } [ **match-order** { **auto** | **config** } ] command to create a named advanced ACL and enter the advanced ACL view.

  b. Configure rules for the advanced ACL.

     Run the **rule** command to configure a rule with the **tcp-flag** parameter specified.

     For example, it is required that users on network segment 192.168.1.0/24 can access network segment 192.168.2.0/24, but users on network segment 192.168.2.0/24 cannot access network segment 192.168.1.0/24.

     From TCP connection setup to teardown only the packets used for TCP connection establishment can have the ACK value of 1 and RST value of

 Copyright © Huawei Technologies Co., Ltd. 

1. According to this characteristic, configure the following ACL rules to permit the packets used for establishing TCP connections and deny other TCP packets on the network segment 192.168.2.0/24. In this way, you can limit the TCP connection requests initiated from this network segment.

- Rule 1: Configure an ACL rule with the **ack** and **rst** keywords specified.

```
rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack  //Permit the TCP packets with the ACK value of 1.
rule 10 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst  //Permit the TCP packets with the RST value of 1.
rule 15 deny tcp source 192.168.2.0 0.0.0.255  //Reject other TCP packets.
```

- Rule 2: Configure an ACL rule with the **established** keyword specified.

```
rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag established  //established indicates that ACK is 1 or RST is 1. The packets exchanged during TCP connection established are permitted.
rule deny tcp source 192.168.2.0 0.0.0.255     //Reject other TCP packets.
```

c. Configure a traffic classifier.

i. Run the **traffic classifier** *classifier-name* [ **operator** { **and** | **or** } ] command in the system view to enter the traffic classifier view.

ii. Run the **if-match acl** { *acl-number* | *acl-name* } command to configure an ACL-based matching rule.

d. Configure a traffic behavior.

Run the **traffic behavior** *behavior-name* command in the system view to create a traffic behavior and enter the traffic behavior view.

e. Configure a traffic action.

There are two actions for packet filtering: **deny** and **permit**. For other traffic actions, see *Huawei AR Series Access Routers Configuration Guide - QoS*.

f. Configure a traffic policy.

i. Run the **traffic policy** *policy-name* command in the system view to create a traffic policy and enter the traffic policy view.

ii. Run the **classifier** *classifier-name* **behavior** *behavior-name* command to configure a traffic behavior for the specified traffic classifier in the traffic policy. That is, bind the traffic behavior to the classifier.

g. Apply the traffic policy.

Run the **traffic-policy** *policy-name* { **inbound** | **outbound** } command in the interface view to apply the traffic policy.

In this example, apply the traffic policy to the inbound direction of the interface connected to network segment 192.168.2.0/24.

- Method 2: Simplified traffic policy

a. Configure an advanced ACL and rules. The configurations are the same as those in traffic policy.

b. Apply the simplified traffic policy.

Run the **traffic-filter** { **inbound** | **outbound** } **acl xxx** command in the interface view to apply the simplified traffic policy (ACL-based packet filtering).

 Copyright © Huawei Technologies Co., Ltd. 

In this example, apply the simplified traffic policy to the inbound direction of the interface connected to network segment 192.168.2.0/24.

## 5.11.5 Which Packets Cannot Be Filtered by the ACL Used by a Traffic Policy?

The ACL used by a traffic policy cannot filter the protocol packets to be sent to the CPU.

- VRRP protocol packets use multicast address 224.0.0.18 as the destination address. The VRRP protocol packets are sent to the CPU for processing; therefore, the ACL in a traffic policy does not take effect on these packets. Member routers in a VRRP group negotiate the master switch using the VRRP protocol packets.
- DHCP clients exchange DHCP packets with the DHCP server to obtain valid IP addresses. The DHCP packets are sent to the CPU for processing; therefore, the ACL in a traffic policy does not take effect on these packets. The device cannot use ACLs to prevent users connected to interfaces from obtaining IP addresses through DHCP.
- When a host pings a device, the ICMP packet is sent to the CPU of the device for processing; therefore, the ACL in a traffic policy does not take effect on the ICMP packet. The device cannot use ACLs to block ping packets from hosts.

To filter the protocol packets to be sent to the CPU, you can apply an ACL to the blacklist configured in the local attack defense policy. The configuration procedure is as follows:

1. Run the **cpu-defend policy** *policy-name* command in the system view to create an attack defense policy.
2. Run the **blacklist** *blacklist-id* **acl** *acl-number* command to create a blacklist.
3. Run the **cpu-defend-policy** *policy-name* [ **global** | **slot** *slot-id* ] to apply the attack defense policy.

## 5.11.6 How Are deny and permit Actions in ACL Rules Used in Different Services?

The deny and permit actions in ACL rules have different functions in different services.

- Traffic policy
  a. When **permit** is used in the ACL rule, the system executes the specified traffic behavior only when traffic matches the ACL rule. When the traffic behavior is **deny**, the system discards traffic matching the rule. When the traffic behavior is **permit**, the system forwards traffic matching the rule.
  b. When **deny** is used in the ACL rule, the system discards packets when traffic matches the ACL rule, and the action in the traffic behavior does not take effect (except traffic statistics collection and traffic mirroring actions).
  c. If an ACL does not contain rules, the traffic policy referencing the ACL does not take effect.

 Copyright © Huawei Technologies Co., Ltd. 

- Simplified traffic policy
  a. When **permit** is used in the ACL rule, the system executes the behavior in the simplified traffic policy, for example, allowing the matching packets to pass and limiting the rate of matching packets.
  b. When **deny** is used in the ACL rule and the ACL is applied to simplified traffic policy, the system discards the packets matching the ACL rule.
  c. If an ACL does not contain rules, the simplified traffic policy using the ACL does not take effect.
- IPSec
  a. When **permit** is used in the ACL rule, the system uses IPSec policies to protect traffic matching the ACL rule, and then forwards the traffic.
  b. When **deny** is used in the ACL rule, the system discards the packets matching the ACL rule.
  c. When the ACL does not contain rules, the IPSec policy referencing the ACL does not take effect. That is, the system forwards the packets passing the interface without performing any other operation.
- Firewall
  a. When **permit** is used in the ACL rule:
     - When the ACL is applied to the **inbound** traffic, the system forwards the packets matching the ACL rule sent from the low-priority zone to the high-priority zone.
     - When the ACL is applied to the **outbound** traffic, the system forwards the packets matching the ACL rule sent from the high-priority zone to the low-priority zone.
  b. When **deny** is used in the ACL rule:
     - When the ACL is applied to the **inbound** traffic, the system discards the packets matching the ACL rule sent from the low-priority zone to the high-priority zone.
     - When the ACL is applied to the **outbound** traffic, the system discards the packets matching the ACL rule sent from the high-priority zone to the low-priority zone.
  c. When the ACL does not contain rules:
     - When the ACL is applied to the **inbound** traffic, the ACL does not take effect, and the system discards all packets sent from the low-priority zone to the high-priority zone.
     - When the ACL is applied to the **outbound** traffic, the ACL does not take effect, and the system allows all packets sent from the high-priority zone to the low-priority zone.
- NAT
  a. When **permit** is used in the ACL rule, the system uses the address pool to translate addresses for the packets of which the source IP address is specified in the ACL rule.

 Copyright © Huawei Technologies Co., Ltd. 

b. When **deny** is used in the ACL rule or the ACL does not contain rules, the NAT policy referencing the ACL does not take effect. That is, the system searches routes for packets, but does not translate addresses.

- Telnet
  a. When **permit** is used in the ACL rule:
     - When the ACL is applied to the **inbound** traffic, only the devices matching the ACL rule can access the local device.
     - When the ACL is applied to the **outbound** traffic, the local device can access other devices matching the ACL rule.
  b. When **deny** is used in the ACL rule:
     - When the ACL is applied to the **inbound** traffic, the devices matching the ACL rule cannot access the local device.
     - When the ACL is applied to the **outbound** traffic, the local device cannot access the devices matching the ACL rule.
  c. When the ACL contains rules but the packets from other devices do not match the ACL rules:
     - When the ACL is applied to the **inbound** traffic, other devices cannot access the local device.
     - When the ACL is applied to the **outbound** traffic, the local device cannot access other devices.
  d. When the ACL does not contain rules:
     - When the ACL is applied to the **inbound** traffic, any device can access the local device.
     - When the ACL is applied to the **outbound** traffic, the local device can access any device.
- HTTP
  a. When **permit** is used in the ACL rule, another device with the specified source IP address can set up an HTTP connection with the local device.
  b. When **deny** is used in the ACL rule, other devices cannot set up HTTP connections with the local device.
  c. When the ACL contains rules but the packets from other devices do not match the ACL rules, other devices cannot set up HTTP connections with the local device.
  d. When the ACL does not contain rules, any device can set up an HTTP connection with the local device.
- FTP
  a. When **permit** is used in the ACL rule, another device with the specified source IP address can set up an FTP connection with the local device.
  b. When **deny** is used in the ACL rule, other devices cannot set up FTP connections with the local device.
  c. When the ACL contains rules but the packets from other devices do not match the ACL rules, other devices cannot set up FTP connections with the local device.

 Copyright © Huawei Technologies Co., Ltd. 

d. When the ACL does not contain rules, any device can set up an FTP connection with the local device.

- TFTP
  a. When **permit** is used in the ACL rule, the local device can set up a TFTP connection with the device with the specified source IP address.
  b. When **deny** is used in the ACL rule, the local device cannot set up a TFTP connection with any device.
  c. When the ACL contains rules but the packets from other devices do not match the ACL rules, other devices cannot set up TFTP connections with the local device.
  d. When the ACL does not contain rules, the local device can set up TFTP connections with any devices.
- SNMP
  a. When **permit** is used in the ACL rule, the NMS with the specified source IP address can access the local device.
  b. When **deny** is used in the ACL rule, no NMS can access the local device.
  c. When the ACL does not contain rules, any NMS can access the local device.
- NTP
  a. When **permit** is used in the ACL rule, the access control right configured in **ntp-service access** takes effect.
  b. When **deny** is used in the ACL rule, the access control right configured in **ntp-service access** does not take effect.
  c. When the ACL does not contain rules, the access control right configured in **ntp-service access** does not take effect.

 Copyright © Huawei Technologies Co., Ltd. 

# 6 Firewall Configuration

## About This Chapter

6.1 Overview of Firewalls
6.2 Understanding Firewalls
6.3 Application Scenarios for Firewalls
6.4 Licensing Requirements and Limitations for Firewalls
6.5 Default Settings for Firewalls
6.6 Configuring Basic Functions of the Firewall
6.7 Configuring the Packet Filtering Firewall
6.8 Configuring Stateful Firewall (ASPF)
6.9 Configuring the Blacklist
6.10 Configuring the Whitelist
6.11 Configuring Port Mapping
6.12 Configuring Attack Defense
6.13 Configuring Traffic Statistics and Monitoring
6.14 Configuring the Firewall Log Function
6.15 Configuring Virtual Firewalls
6.16 Configuring Firewalls in HSB Mode
6.17 Maintaining the Firewall
6.18 Configuration Examples for Firewalls
6.19 FAQ About Firewalls

 Copyright © Huawei Technologies Co., Ltd. 

# 6.1 Overview of Firewalls

## Definition

A firewall separates an internal network from external networks to protect the internal network from unauthorized access.

## Purpose

A firewall provides the following functions:

- Prevents hazards on external networks from spreading to internal networks.
- Protects devices and key resources on internal networks.
- Controls internal users' access to external networks.

# 6.2 Understanding Firewalls

## 6.2.1 Security Zone and Interzone

Firewall functions are implemented based on security zones and interzones.

### Security Zone

A security zone (zone for short) is an interface or a group of interfaces with the same security attributes. Each zone has a globally unique security priority.

The firewall considers data flows transmitted within a zone reliable and implements no security policy for these data flows. It checks security and implements security policies for data flows transmitted from one zone to another.

### Interzone

Any two zones form an interzone, which has an independent interzone view. Most firewall configurations are performed in the interzone view.

For example, zone1 and zone2 form an interzone. You can configure an ACL-based packet filter in the interzone view to filter data flows transmitted between zone1 and zone2.

After the firewall is enabled in an interzone, when a user in the high-priority zone connects to the low-priority zone, the firewall records information such as the IP address and VPN in the request packet and generates a session. When receiving the response packet, the firewall checks the packet information. Because the packet information has been recorded in the session table, the firewall allows the response packet to pass. By default, a user in the low-priority zone cannot connect to the high-priority zone. To allow internal users to access the external network and prevent external users from accessing the internal network, configure the internal network as a high-priority zone and the external network as a low-priority zone.

 Copyright © Huawei Technologies Co., Ltd. 

### Advantages of the Zone-based Firewall

On traditional switches and routers, policies are configured based on inbound or outbound interfaces. As the firewall technology develops, a firewall controls communication between an internal network, an external network, and a demilitarized zone (DMZ). Interface-based policy configuration increases workload of the network administrator, and incorrect configurations bring security risks.

Some firewalls support global security policy configuration. This configuration method does not allow different security policies on interfaces or zones, which limit application of firewalls.

Compared with interface based and global configuration, zone-based firewall configuration adds a group of interfaces to security zones and applies security policies to zones, simplifying configuration while maintaining flexibility. Zone-based firewall configuration reduces workload of the network administrator and allows different security policies to be applied in complex networking.

## 6.2.2 Firewall Working Mode

To improve networking flexibility, a firewall device defines the working mode of each interface but not the entire device. An interface has the following modes.

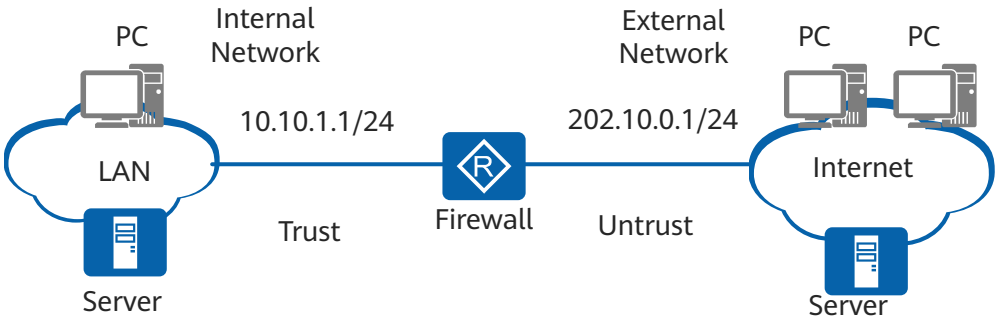
### Routed Mode

A device is located between the internal network and the external network. On the device, the interfaces connecting to internal network and external network are assigned IP addresses on different network segments. The network topology needs to be changed.

As shown in **Figure 6-1**, two zones are configured on the device, Trust zone and Untrust zone. The interface in the Trust zone is connected to the internal network, and the interface in the Untrust zone is connected to the external network.

Note that, the interfaces in the Trust zone and Untrust zone locate in different subnets.

**Figure 6-1** Networking diagram of routed mode




When forwarding packets among the interfaces in Layer 3 zones, the device searches the routing table according to IP addresses of packets. The device is similar to a router in this case. However, unlike a router, the device filters the packets and determines whether to allow them to pass according to the session table or ACL rules. In addition, the firewall takes other attack defense measures.

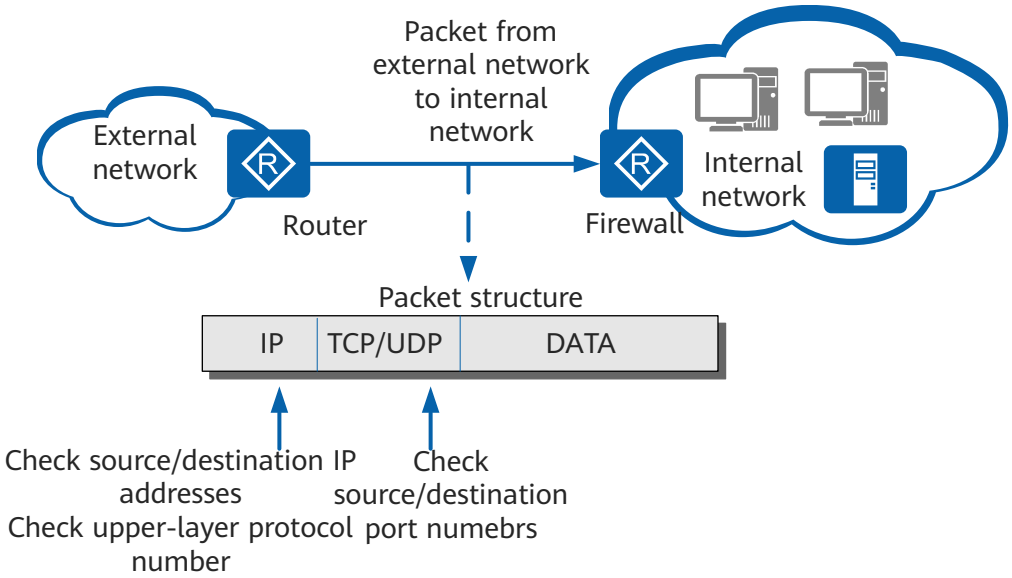
 Copyright © Huawei Technologies Co., Ltd. 

## 6.2.3 Packet Filtering Firewall

A packet filtering firewall uses access control lists (ACLs) to filter packets based on the upper-layer protocol ID, source and destination IP addresses, source and destination port numbers, and packet transmission direction.

When receiving an IP datagram, the firewall obtains the packet header, and then compares the packet header information with ACL rules to determine whether to forward or discard the IP datagram. **Figure 6-2** shows how packet filtering is implemented on the firewall.

**Figure 6-2** Packet filtering firewall




### Packet Filtering Firewall on the Device

The device supports packet filtering firewall and can filter the following packets:

- Common IP packets: The firewall checks the source and destination IP addresses, source and destination port numbers, and protocol IDs of IP packets against an ACL. It forwards the packets permitted by the ACL and discards the packets denied by the ACL. The information that the firewall checks is contained in the IP, TCP, or UDP header.
- Fragment packets: The firewall can identify the packet types, including non-fragment packets, initial fragment packets, and non-initial fragment packets.

  When receiving the initial fragment of a packet, the firewall compares Layer 3 and Layer 4 information of the initial fragment with the ACL. If the fragment is permitted by the ACL, the firewall records information about this fragment and creates a matching table for the following fragments. When the following fragments arrive, the firewall directly forwards them according to the matching table.

  In addition, the firewall has a default method to process the packets that do not match the ACL. The default method can be set by users.

## 6.2.4 Stateful Firewall

A packet filtering firewall is a static firewall and has the following problems:


Copyright © Huawei Technologies Co., Ltd.

- Some security policies cannot be configured for multi-channel application-layer protocols such as FTP and SIP.
- Some attacks (such as TCP SYN and Java Applets) from the transport and application layers cannot be detected.
- ICMP attacks cannot be prevented because bogus ICMP error packets cannot be identified.
- The first packet of TCP connections must be an SYN packet. If the first packet of a TCP connection is not an SYN packet, the packet is discarded. When a firewall device connects to a network for the first time, non-first packets of existing TCP connections are all discarded if they pass through the new firewall, and the TCP connections are torn down.

Application specific packet filter (ASPF), a stateful firewall, is introduced to solve the preceding problems. ASPF can detect attacks related to the following protocols:

- Application-layer protocols, including File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Session Initiation Protocol (SIP) and Real Time Streaming Protocol (RTSP)
- Transport-layer protocols, including TCP and UDP

## ASPF Functions

Major functions:

- Checks application-layer protocol information, such as the protocol type and port number, and monitors the connection-based application-layer protocol status. ASPF maintains status information of each connection and uses the status information to determine whether to forward or discard data packets.
- Checks transport-layer protocol information and determines whether to forward or discard TCP or UDP packets based on the source IP address, destination IP address, and port number.

Additional functions:

- Checks contents of application-layer packets.
- Checks the first packet of a TCP connection.
- Filters ICMP error packets. An ICMP error packet carries information about a connection. If information in an ICMP error packet matches no connection, ASPF determines whether to discard the packet based on the current configuration.

The ASPF function and the packet filtering firewall can be used together on network edges to provide more comprehensive security policies on an enterprise's internal network.

## Basic Concepts of ASPF

- Single-channel protocol

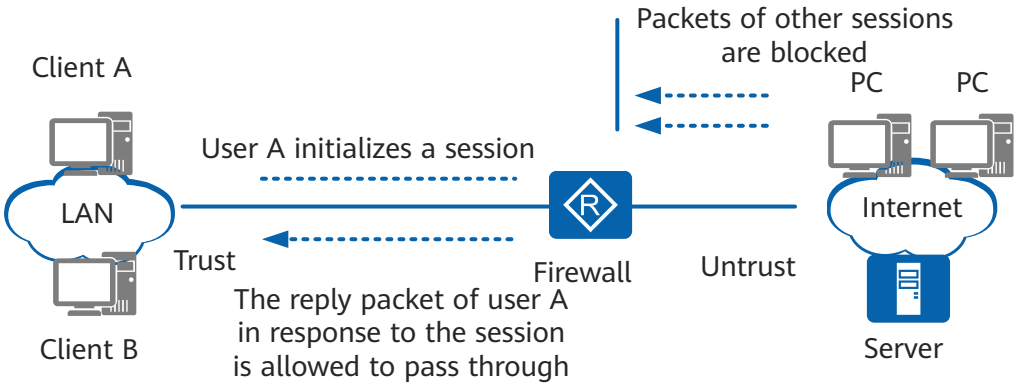
  A single-channel protocol uses only one channel to exchange from session setup to deletion. An example is HTTP.
- Multi-channel protocol

 Copyright © Huawei Technologies Co., Ltd. 

A multi-channel protocol uses a control channel to exchange control information and several control channels to exchange data. An example is FTP or RTSP.

## Basic Principle of Application-Layer Protocol Detection

**Figure 6-3** Basic principle of application-layer protocol detection




As shown in **Figure 6-3**, an ACL is configured on the device to allow internal hosts to access external networks but reject access from external networks, which ensures internal network security. However, the ACL will filter out reply packets sent in response to connection requests, leading to connection failures.

After application-layer protocol detection is configured on the router, ASPF monitors each application-layer session and creates a status entry and a temporary access control list (TACL).

1. ASPF creates a status entry when detecting the first packet sent to an external network. The status entry maintains the status of a session at a specified time and checks whether the session status transition is correct.
2. A TACL is created when a status entry is created and is deleted after the session is disconnected. A TACL is an extended permit item of the ACL. A TACL matches all reply packets in a session and helps set up a temporary return channel on the external interface of the firewall for reply packets.

The following uses FTP as an example to describe the multi-channel protocol detection process.

**Figure 6-4** FTP detection process

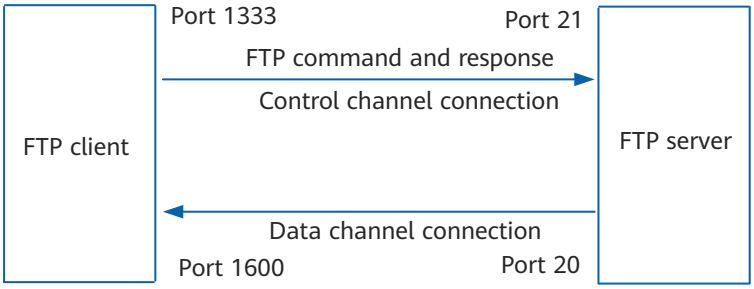



**Figure 6-4** shows the FTP connection setup process. Assume that the FTP client uses port 1333 to initiate an FTP control channel connection to port 21 on the FTP

 Copyright © Huawei Technologies Co., Ltd. 

server. After negotiation, the FTP server uses port 20 to initiate a data channel connection to port 1600 on the FTP client. If data transmission times out or ends, the connections are deleted.

The FTP detection process is as follows:

1. Check whether IP packets sent from the outbound interface are TCP-based FTP packets.
2. Check the port number and verify that the connection is a control connection. Create a status entry and TACL for the reply packets.
3. Check FTP control connection packets, resolve FTP commands, and update the status entry based on the commands. If there is a data channel setup command, create a TACL for the data connection. The firewall does not perform status detection on data connections.
4. Perform matching check on reply packets based on the protocol type. Determine whether to allow reply packets to pass based on the status entry and TACL.
5. Delete the status entry and TACL when the FTP connection is deleted.

The process for detecting single-channel application layer protocols is simple. When a connection is initiated, the firewall creates a TACL. When the connection is deleted, the firewall deletes the TACL.

### Basic Principle of Transport-Layer Protocol Detection

Transport-layer protocol detection is common TCP/UDP detection. Different from application-layer protocol detection, transport-layer protocol detection checks transport-layer information in packets, such as the source address, destination address, and port number. In common TCP/UDP detection, reply packets returned to the external interface of ASPF must exactly match the packet sent from the interface. That is, the source address, destination address, source port and destination port of the reply packet must be the same as the destination address, source address, destination port, and source port of the packet sent from the interface. Otherwise, reply packets are rejected. If you configure TCP detection without application-layer protocol detection for multi-channel application layer protocols (such as FTP), data connections cannot be set up.

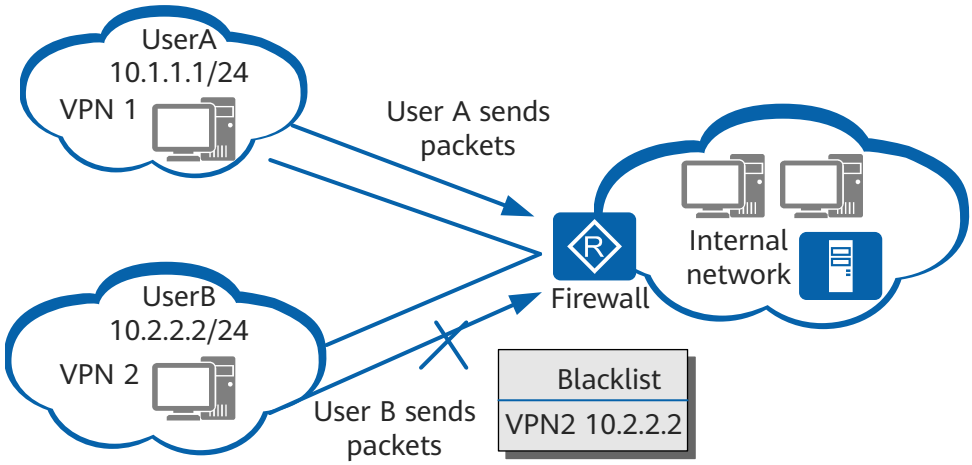
## 6.2.5 Blacklist

A blacklist filters packets based on source VPNs and source IP addresses. Compared with ACLs, the blacklist uses simpler matching rules and therefore can filter packets at a higher speed. The blacklist can effectively block the packets sent from specific IP addresses. Blacklist entries can be manually configured or dynamically generated.

As shown in **Figure 6-5**, the IP address of user B is in the blacklist, so packets from user B are discarded by the firewall.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 6-5** Blacklist




### Blacklist Features Supported by the Device

You add entries to the blacklist manually. In addition, if the device detecting an IP sweeping attack or port scanning attack, it adds the attacking IP address or port to the blacklist. Then, all the packets from this IP address or port are rejected within a certain period. You can set an aging time for entries in the blacklist.

The firewall discards all the packets from the blacklisted IP addresses no matter whether the packets are permitted by the ACL.

You can export entries in a blacklist to a file or import entries to a blacklist from a file.

## 6.2.6 Whitelist

IP addresses in the whitelist will not be added to the blacklist statically or dynamically. An entry in the whitelist is represented by a source VPN and a source IP address, and must be manually configured.

If valid service packets sent from some devices are similar to IP sweeping attack or port scanning attack packets, you can add these devices to the whitelist so that packets sent from the devices will not be discarded by the firewall.

### Functions of Whitelist

If you add the VPN or IP address of a host to the whitelist, the firewall does not check packets sent from the host for IP sweeping or port scanning attack, and does not add the IP address of the host to the blacklist.


Copyright © Huawei Technologies Co., Ltd.

### Whitelist Features Supported by the Device

After receiving a packet, the device checks whether the packet is sent from an IP address in the whitelist. If the packet is sent from an IP address in the whitelist, the device does not check the packet for IP sweeping or port scanning attack, or add the IP address to the blacklist. However, the device still performs other security checks, such as ACL-based packet filtering, ASPF, and traffic statistics and monitoring, to ensure network security.

You can set an aging time for whitelist entries.

You can export whitelist entries to a file or import entries to a whitelist from a file.

## 6.2.7 Port Mapping

The application-layer protocols use well-known ports for communication. Port mapping allows you to define new port numbers for different applications or specify the range of hosts that use non-well-known port numbers.

Port mapping applies to service-sensitive features such as application specific packet filter (ASPF) and Network Address Translation (NAT). For example, the FTP server 10.10.10.10 on an enterprise intranet provides the FTP service through port 2121. When accessing the FTP server through a NAT server, users must use port 2121. By default, port 21 is used for FTP packets. The FTP server cannot identify the FTP packets that use port 21. In this case, you need to map port 2121 to the FTP protocol. After port mapping, the NAT server can identify the FTP packets that use port 2121 and send the FTP packets to the FTP server. In this way, users can access the FTP server.

The device provides ACL-based port mapping and performs port mapping only for the packets matching the specified ACL. Port mapping employs basic ACLs (2000 to 2999). In ACL-based packet filtering, the device matches the destination IP addresses of the packets with the IP address in the basic ACL rules.

As shown in **Figure 6-6**, the PC on the external network accesses the WWW server (port 8080) on the internal network. When the device receives packets sent by the PC, it matches the packets with the ACL. Only packets with the destination IP address 10.38.2.4 can pass through the device.

**Figure 6-6** Port mapping diagram




## 6.2.8 Attack Defense

Attack defense is an important network security function of the firewall. With this function, the firewall can detect various network attack behaviors and take measures to protect the network, ensuring normal running of the internal network and systems.

 Copyright © Huawei Technologies Co., Ltd. 

## Types of Network Attacks

Network attacks are classified into three types: Denial of Service (DoS) attacks, scanning and snooping attacks, and malformed packet attacks.

- DoS attack

  An attacker sends a large number of data packets to the target system to prevent the system from processing requests from authorized users or make the host stop responding. DoS attackers include SYN Flood attacks and Fraggle attacks.

  DoS attacks are different from other attacks because DoS attackers do not search for the ingress of a network but prevent authorized users from accessing resources or firewall.

- Scanning and snooping attack

  Scanning and snooping attacks identify existing systems on a network through ping scanning (including ICMP and TCP scanning), and then find out potential targets. By scanning TCP and UDP ports, the attackers can know the operating system and the monitored services.

  Through scanning and snooping, an attacker can generally know the service type of the system and prepare for further intrusion to the system.

- Malformed packet attack

  An attacker sends malformed IP packets to a target system. The target system crashes when processing the malformed IP packets. Malformed packet attacks include Ping of Death and Teardrop.

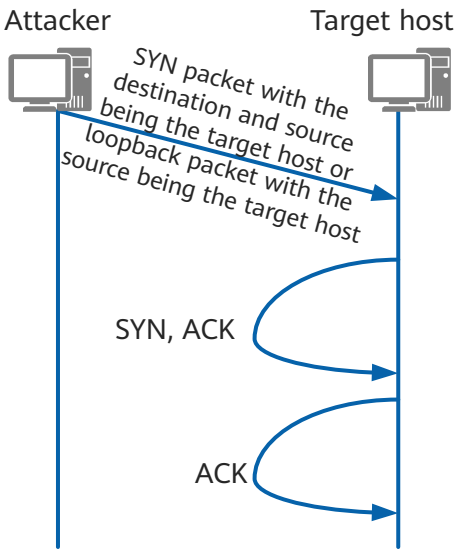
The following describes typical attacks on networks.

## Land Attack

An attacker initiates a Land attack by setting the source and destination addresses of a TCP SYN packet to the IP address of a target host. The target host then sends a SYN-ACK message to its own IP address, and the ACK message is sent back to the target host. This forms a null session. Every null session exists until it times out. **Figure 6-7** shows a Land attack.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 6-7** Land attack



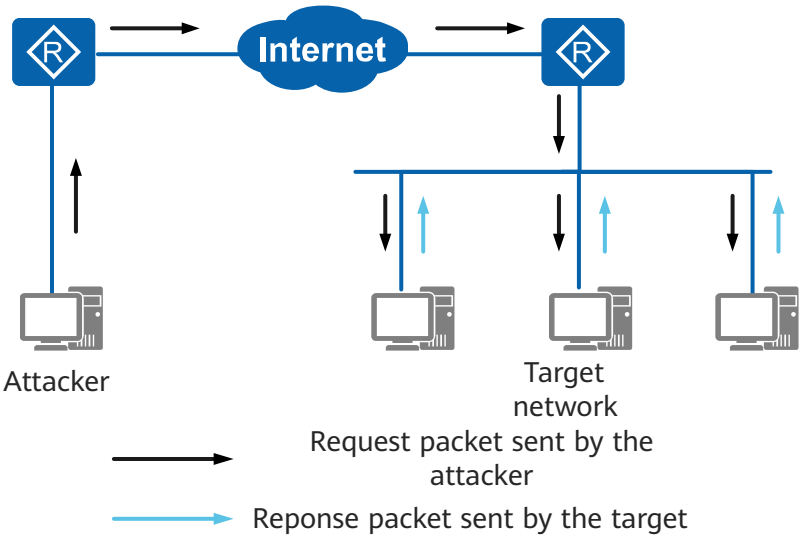

The responses to the Land attack vary according to the targets. For instance, many UNIX hosts crash while Windows NT hosts slow down.

## Smurf Attack

A simple Smurf attack is used to attack a network. The attacker sends an ICMP Echo request to the broadcast address of the network. All the hosts on the network respond to the request and the network is congested. **Figure 6-8** shows a simple Smurf attack.

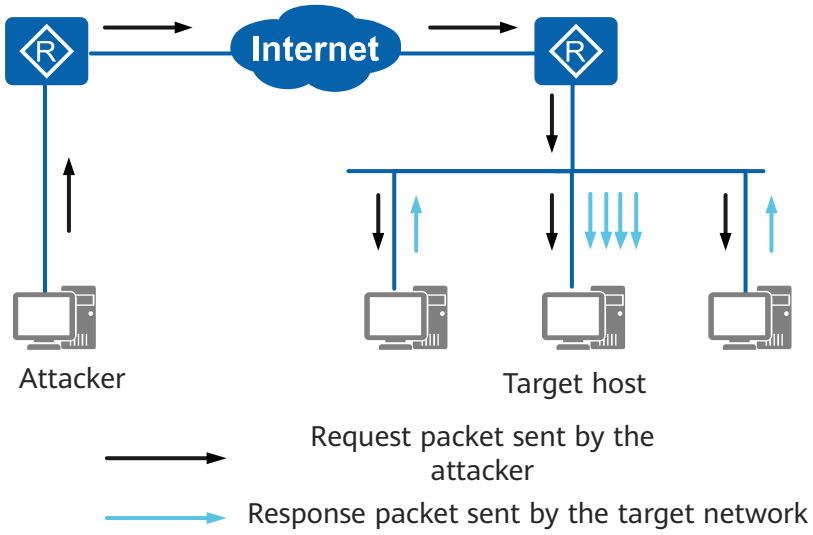

Copyright © Huawei Technologies Co., Ltd.

**Figure 6-8** Simple Smurf attack




An advanced Smurf attack targets hosts. The attacker sends an ICMP Echo request packet to the network where the target host is located. The source IP address of the packet is the IP address of the target host; therefore, all ICMP Echo Reply packets are sent to the target host. This slows down packet processing on the target host or can even make the host crash. **Figure 6-9** shows an advanced Smurf attack.

**Figure 6-9** Advanced Smurf attack





Copyright © Huawei Technologies Co., Ltd.

Sending attack packets generates certain traffic and lasts for some time. Theoretically, the attack causes severe damages when there are more hosts on the network.

## WinNuke Attack

Network Basic Input/Output System (NetBIOS) is a network access interface that is widely used in file sharing, print sharing, and data exchange between different operating systems. Generally, NetBIOS is a multicast-based interface and runs over the Logical Link Control Type 2 (LLC2) protocol. The common TCP/UDP ports to implement NetBIOS on the TCP/IP protocol stack:

- 139: a TCP port used for the NetBIOS sessions.
- 137: a UDP port used for the NetBIOS name service.
- 136: a UDP port used for the NetBIOS datagram service.

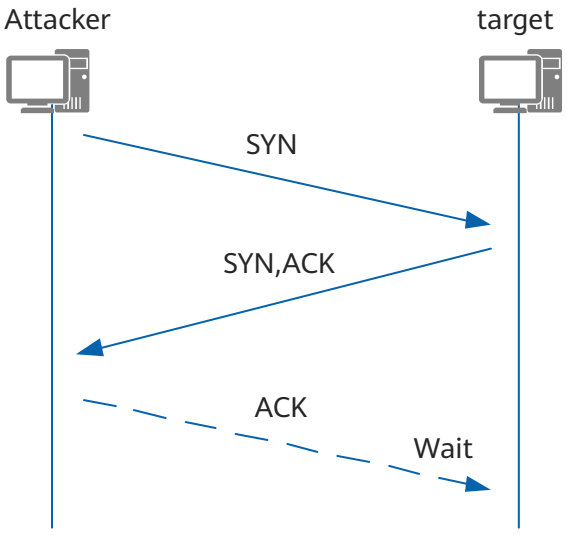
Windows operating systems implement NetBIOS over TCP/IP and open port 139.

WinNuke attacks use the vulnerability of Windows operating systems. An attacker sends data packets carrying TCP out-of-band (OOB) packets to port 139. These attack packets differ from normal OOB packets in that the pointer field in the packets does not match the actual location of data. When the Windows operating system processes these packets, it may crash.

## SYN Flood Attack

A SYN Flood attack uses the three-way handshake mechanism of the TCP protocol to attack the target host. An attacker sends a SYN packet to the target host to request for a TCP connection, but it does not respond to the SYN-ACK packet sent from the target host. If the target host does not receive the response from the attacker, it keeps waiting and forms a half connection. **Figure 6-10** shows a SYN Flood attack.

**Figure 6-10** Half connection




 Copyright © Huawei Technologies Co., Ltd. 

The attacker sends a lot of TCP SYN packets to make the target host set up many half connections, which occupy a large number of resources. When the resources on the target host are used up, data processing on the host slows down and authorized users cannot access the host.

The attacker can also generate a SYN packet with a pseudo or non-existent source address to attack the target host.

## ICMP Flood Attack

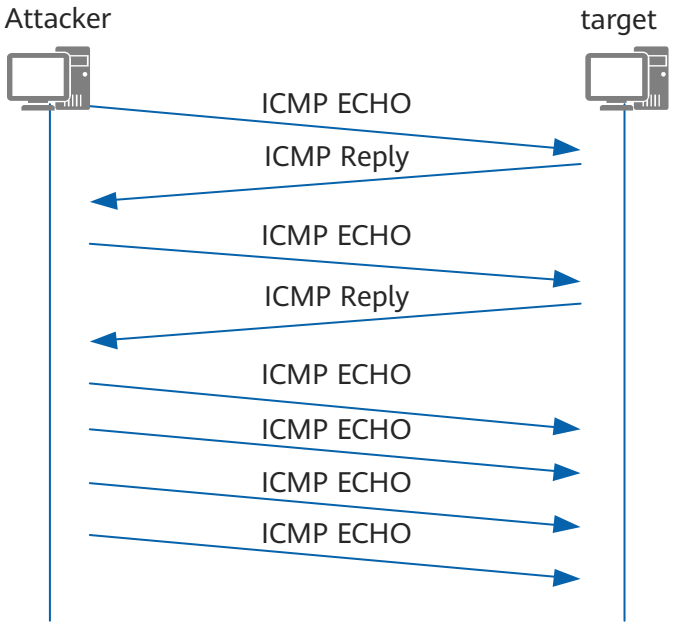
A network administrator uses the ping program to monitor networks and locate faults. The ping process is as follows:

1. A source host sends an ICMP Echo Request packet to a destination host.
2. After receiving the ICMP Echo Request packet, the destination host returns an ICMP Echo Reply packet to the source host.

ICMP packets are processed by the CPU and may consume many CPU resources in some cases.

If an attacker sends a large number of ICMP Echo Request packets to a target host, the target host becomes busy processing these Echo Request packets and cannot process other data packets. **Figure 6-11** shows an ICMP Flood attack.

**Figure 6-11** ICMP Flood attack




## UDP Flood Attack

A UDP flood attack is similar to an ICMP flood attack. An attacker sends a large number of UDP packets to a target host. The target host becomes busy processing these UDP packets and cannot process normal data packets.

 Copyright © Huawei Technologies Co., Ltd. 

## IP Sweeping and Port Scanning Attack

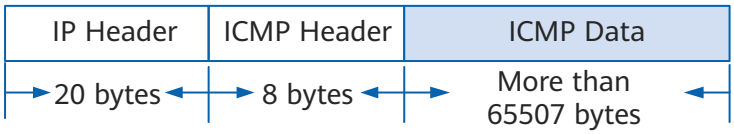
An attacker uses a scanning tool to probe target IP addresses and ports. The targets then respond to the probes, through which the attacker can know which target systems are active and connected to the network and which ports are open or closed.

## Ping of Death Attack

Ping of Death is an attack to a system by sending oversized ICMP packets.

The Length field of an IP packet is 16 bits, indicating that the maximum length of an IP packet is 65535 bytes. If the data field of an ICMP Echo Request packet is longer than 65507 bytes, the length of the ICMP Echo Request packet (ICMP data + 20-byte IP header + 8-byte ICMP header) is larger than 65535 bytes. Some systems or devices cannot process oversized ICMP packets. If they receive such packets, they may stop responding, crash, or restart. **Figure 6-12** shows an oversized ICMP packet.

**Figure 6-12** Oversized ICMP packet




## Large-ICMP Attack

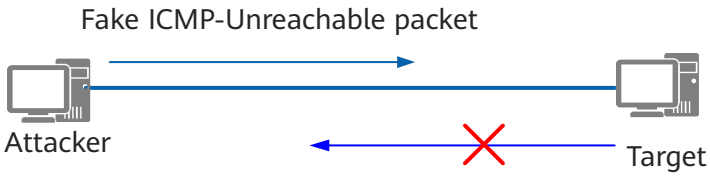
Similar to a Ping of Death attack, a Large-ICMP attack sends oversize ICMP packets to attack a system. Although the length of Large-ICMP packets does not exceed the maximum length of an IP packet (65535 bytes), the Large-ICMP packets also have great impact on some operating systems.

To prevent Large-ICMP attack, set the maximum length of ICMP packets on the firewall.

## ICMP-Unreachable Attack

After receiving an ICMP network-unreachable packet (packet type field is 3 and code is 0) or host-unreachable packet (packet type is 3 and code is 1), some systems consider the subsequent packets sent to this destination unreachable. The systems then disconnect the destination from the host. **Figure 6-13** shows an ICMP-Unreachable attack.

**Figure 6-13** ICMP-unreachable attack





Copyright © Huawei Technologies Co., Ltd.

The attacker sends ICMP-Unreachable packets to the target hosts to change routes on the target hosts. In this case, packet forwarding on the hosts is abnormal.

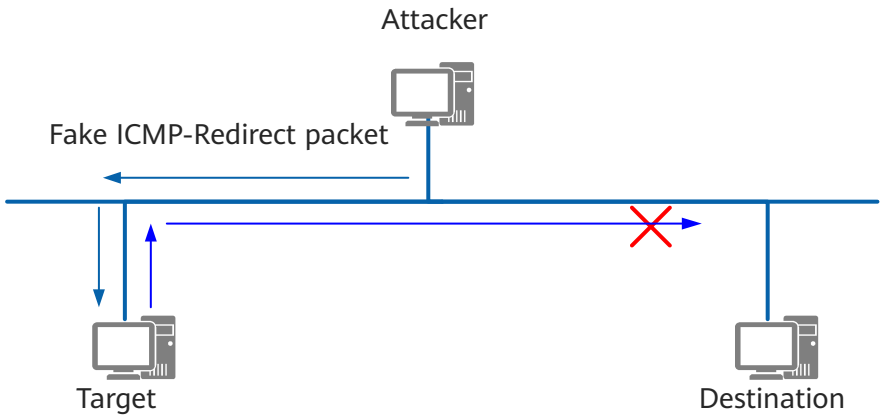
## ICMP-Redirect Attack

An ICMP-Redirect attack is similar to an ICMP-Unreachable attack.

A network device can send ICMP Redirect packets to a host in the same subnet, requesting the host to change its routes.

Similarly, an attacker sends a fake Redirect packet to the target host on another network segment, requesting the target host to modify the routing table. The attack changes routes on the target host and affects packet forwarding. **Figure 6-14** shows an ICMP-Redirect attack.

**Figure 6-14** ICMP-Redirect attack




## IP Fragment Attack

The fields related to fragmentation of an IP packet are Don't Fragment (DF) bit, More fragments (MF) bit, Fragment Offset, and Length.

If the previous fields conflict and a device does not process the fields properly, the device may stop running or even crash. In the following cases, the fields conflict:

- The DF bit is set, but the MF bit is also set or the fragment offset is not 0.
- The DF bit is 0, but the sum of Fragment Offset and Length is larger than 65535.

In addition, the device must directly discard the fragment packets destined for itself because the fragment packets result in a heavy load in packet caching and reassembly.

## Teardrop Attack

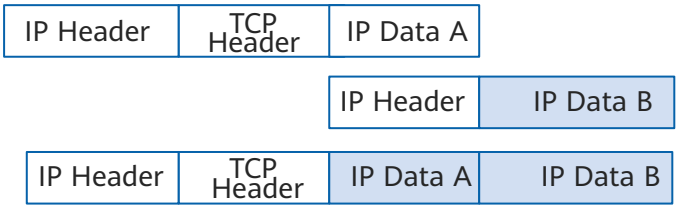
During packet transmission, an IP packet must be fragmented when it is longer than the maximum transmission unit (MTU) of the link layer. The IP packet header contains an offset field and an MF field. If the MF field is set to 1, the IP

 Copyright © Huawei Technologies Co., Ltd. 

packet is a fragment. The offset field indicates the location of this fragment in the whole IP packet. The receiver can reassemble the IP packet based on the information carried in the IP packet header.

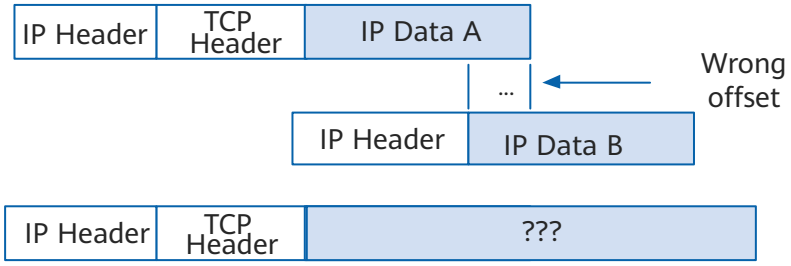
For example, if a large packet is transmitted over a link with a smaller MTU, the packet is fragmented into two IP packets. The receiver then reassembles the two IP packets into the original IP packet. **Figure 6-15** shows the normal packet reassembling process.

**Figure 6-15** Packet reassembly




If an attacker sets the offset field to an incorrect value, the receiver cannot correctly assemble packets. Some TCP/IP protocol stacks may crash when they receive a pseudo fragment containing an overlapping offset. This is a Teardrop attack. **Figure 6-16** shows a Teardrop attack packet.

**Figure 6-16** Teardrop attack diagram




## Fraggle Attack

A Fraggle attack is similar to a Smurf attack, except that the Fraggle attack sends UDP packets but not ICMP packets. Therefore, the Fraggle attack packets can traverse some firewalls that prevent ICMP packets.

A Fraggle attack can be successful because both UDP port 7 (ECHO) and port 19 (Chargen) return responses after receiving UDP packets. The details are as follows:

- UDP port 7 returns a response (similar to the ICMP Echo-Reply packet) after receiving a packet.
- UDP port 19 generates a character flow after receiving the packet.

The two UDP ports send a lot of response packets, which occupy high network bandwidth.

The attacker can send a UDP packet to the target network. The source address of the UDP packet is the IP address of the attacked host and its destination address is the broadcast address or network address of the host's subnet. The destination port number of the packet is 7 or 19. All the hosts with the port open on the

 Copyright © Huawei Technologies Co., Ltd. 

subnet send response packets to the attacked host. This generates heavy traffic, which blocks the network or makes the host crash.

The hosts with the port closed on the subnet generate ICMP Unreachable packets, which still consume high bandwidth. If the attacker sets the source port to 19 (Chargen) and the destination port to 7 (ECHO), severer damages are caused because the response packets are generated automatically and continuously.

### Tracert Attack

Tracert is to discover the packet transmission path through the ICMP timeout packets that is returned when time to live (TTL) value is 0 or through the returned ICMP port-unreachable packets.

An attack can obtain the network structure through Tracert. This brings security risks to the network.

### Malformed TCP Packet Attacks

A malformed TCP packet is a packet with an incorrect 6-bit TCP header. An error will occur when the TCP protocol stack on the receiver processes the TCP packet.

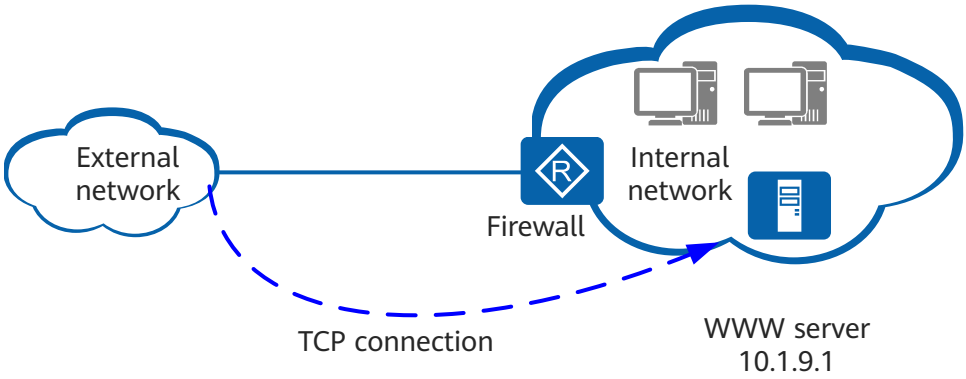
## 6.2.9 Traffic Statistics Collection and Monitoring

A firewall not only monitors data traffic, but also detects the setup of connections between internal and external networks, generates statistics, and analyzes the data. The firewall can use software to analyze the logs after events occur and can also analyze the data in real time.

By checking whether the number of TCP/UDP sessions initiated from external networks to the internal network exceeds the threshold, the firewall decides whether to restrict new sessions from external networks to the internal network or to an IP address in the internal network.

**Figure 6-17** shows an application of the firewall. The IP address-based statistics function is enabled for the packets from external networks to the internal network. If the number of TCP sessions initiated by external networks to web server 10.1.9.1 exceeds the threshold, the firewall device rejects new sessions initiated from the external network until the number of sessions is smaller than the threshold.

**Figure 6-17** Setup of TCP connections




 Copyright © Huawei Technologies Co., Ltd. 

The device supports system-level, zone-level, and IP address-level traffic statistics collection and monitoring.

### System-Level Traffic Statistics Collection and Monitoring

System-level traffic statistics collection and monitoring take effect on all the data flows in interzones with the firewall feature enabled. That is, the firewall device collects statistics about the ICMP, TCP, and UDP sessions in the interzones. When the number of sessions exceeds the threshold, the device restricts the sessions until the number of sessions falls within the threshold.

### Zone-Level Traffic Statistics Collection and Monitoring

The zone-level traffic statistics collection and monitoring take effect on the data flows between zones. That is, the firewall device counts the total number of TCP and UDP sessions between the local zone and other zones. When the number of connections between the local zone and all the other zones or the number of connections in a certain direction exceeds the threshold, the device rejects new sessions until the number of sessions falls within the threshold.

### IP Address-Level Traffic Statistics Collection and Monitoring

The IP address-level traffic statistics collection and monitoring count and monitor the TCP and UDP sessions set up on an IP address in a zone. The firewall device determines whether to restrict the connections in a certain direction by checking whether the number of the TCP or UDP connection requests sent from a source IP address (or received by a destination address) exceeds the threshold. This function prevents DoS caused by the malicious attacks or busy systems.

When the number of TCP and UDP sessions falls below the threshold, the source IP address can initiate sessions and the destination address can receive sessions.

## 6.2.10 Firewall Log

A firewall device records the actions and status of the firewall in real time. For example, the measures taken against IP address spoofing and the detected malicious attacks are recorded in firewall logs.

These logs help you find out the security risks, detect the attempts to violate the security policies, and learn the type of a network attack. The real-time logs are also used to detect the intrusion that is underway.

You can configure the firewall logging function to monitor behaviors and status of the firewall, find security risks, and detect the network attacks and intrusions.

### Firewall Logs Supported by the Device

The device supports the following firewall logs:

- Blacklist logs

  When detecting attacks such as an IP sweeping attack and port scanning attack, the device generates blacklist logs if the blacklist function is enabled.

  A blacklist log is also generated when you add an entry to the blacklist, or when an entry in the blacklist expires.

 Copyright © Huawei Technologies Co., Ltd. 

- Attack logs

  When detecting an attack, the device generates an attack log to record the attack type and parameters.
- Traffic monitoring logs

  When the number of inbound and outbound sessions of the entire system or a zone exceeds the upper threshold or is smaller than the lower threshold, the device generates a log.
- Packet-filter log

  Records information about packet filtering.
- Session logs

  When an entry in the session table expires, the device sends a log to the log server.

## 6.2.11 Virtual Firewall

Increasing small-scale private networks have been established. Most of these private networks belong to small-scale enterprises. Such enterprises require high security and cannot afford a private security device.

The device can be divided into multiple virtual firewalls to serve multiple small-scale private networks.

A virtual firewall integrates a VPN instance and a security instance. It provides a private routing plane and security service for the virtual firewall users.

### VPN Instance

A VPN instance provides separated VPN routes for the users under a virtual firewall. These VPN routes are used to forward the packets received by a virtual firewall.

### Security Instance

A security instance provides separated security services for the users under a virtual firewall. The security instances contain private interfaces, zones, interzones, ACL rules, and NAT rules. They provide the security services such as address binding, blacklist, packet filtering, traffic statistics and monitoring, attack defense, ASPF, and NAT for the users under the virtual firewalls.

## 6.2.12 Firewall in HSB Mode

A firewall is a node that traffic must pass through on a network. If the firewall is faulty, traffic is interrupted. To ensure uninterrupted traffic, prevent firewall single-point failures.

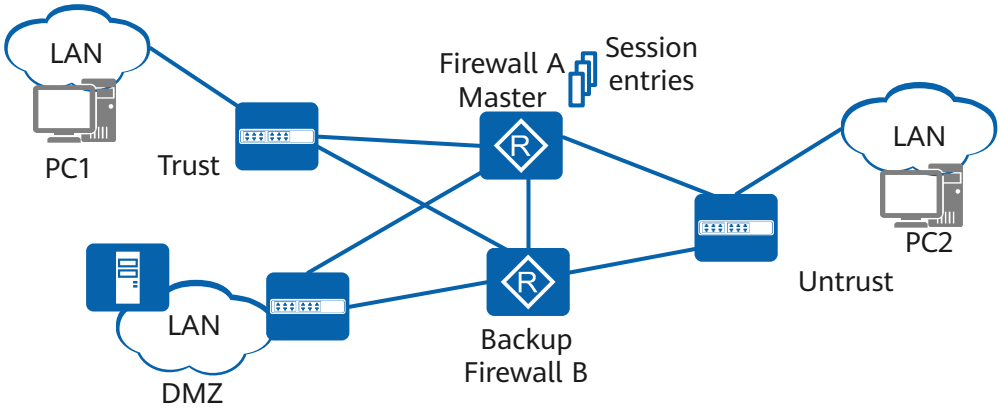
To prevent firewall single-point failures, deploy two firewalls in hot standby (HSB) mode. One functions as the master firewall, and the other functions as the backup firewall. Interfaces on the master and backup firewalls connect to corresponding security zones. The Virtual Router Redundancy Protocol (VRRP) determines the master and backup firewalls. The firewall session entry synchronization is performed using HSB.

 Copyright © Huawei Technologies Co., Ltd. 

## Firewall in HSB Mode

The firewall is a stateful firewall that checks only the first packet in a session and dynamically generates session entries. A session entry records the status of a session. Only subsequent packets (including response packets) that match the session entry can pass through the firewall.

**Figure 6-18** Networking diagram of firewalls in HSB mode




As shown in **Figure 6-18**, Firewall A functions as the master firewall that traffic must pass through. Firewall B is in backup state and no traffic pass through it.

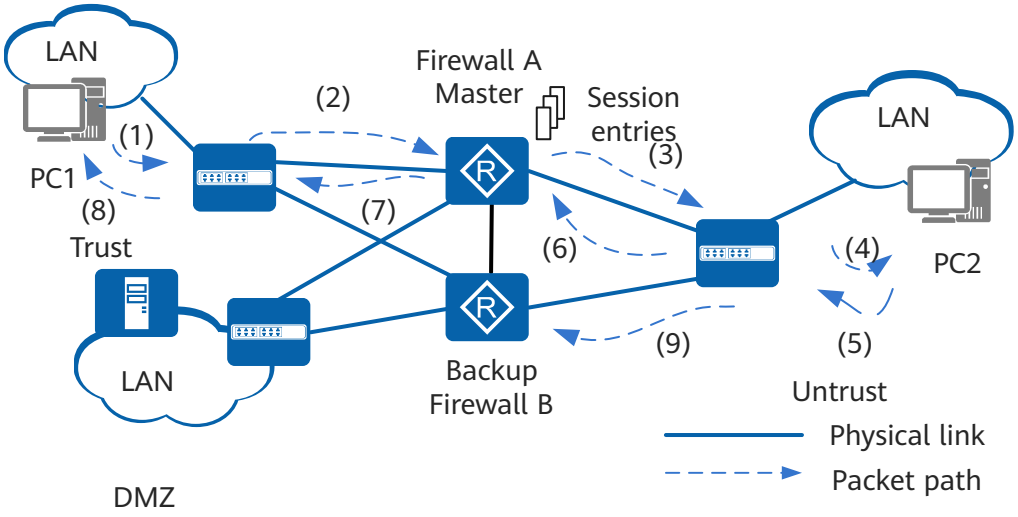
If Firewall A is faulty or links are faulty, traffic is switched to Firewall B. Before master/backup switchover, if session entries are not backed up on Firewall B, previous sessions that pass through Firewall A match no entry on Firewall B and are interrupted.

To ensure that the backup firewall takes over the work of the master firewall smoothly when the master firewall is faulty, back up session entries and status information between the master firewall and the backup firewall in real time. Currently, session entries and status information between the master firewall and the backup firewall are backed up using HSB.


Copyright © Huawei Technologies Co., Ltd.

## Interface Status Requirement

**Figure 6-19** Packets forwarding routes




On a firewall, interfaces that connect to security zones must be in the same state, that is, all interfaces are in master or backup state at the same time.

As shown in **Figure 6-19**:

- Assume that all interfaces on Firewall A are in master state, and all interfaces on Firewall B are in backup state. PC1 in Trust zone connects to PC2 in Untrust zone. Packets are forwarded along (1) > (2) > (3) > (4). When forwarding the access packet, Firewall A dynamically generates a session entry. The response packet sent from PC2 is forwarded along (5) > (6) > (7) > (8). When reaching Firewall A, the response packet can match the session entry and passes through Firewall A. Communication between Firewall A and Firewall B is successful.
- Assume that interfaces on Firewall B that connect to Trust zone are in backup state, but interfaces that connect to Untrust zone are in master state. When a packet sent from PC1 passes through Firewall A and reaches PC2, Firewall A dynamically generates a session entry. The response packet sent from PC2 is forwarded along (5) > (9), and reaches Firewall B. No matched session entry is recorded on Firewall B. If the response packet is not allowed based on other rules, Firewall B discards the packet, and communicate is interrupted.

Smart Link ensures the stability of links connected to switches. A directly connected link is deployed between the master and backup firewalls to ensure that traffic is forwarded to the peer firewall when a link is faulty.


Copyright © Huawei Technologies Co., Ltd.

NOTE

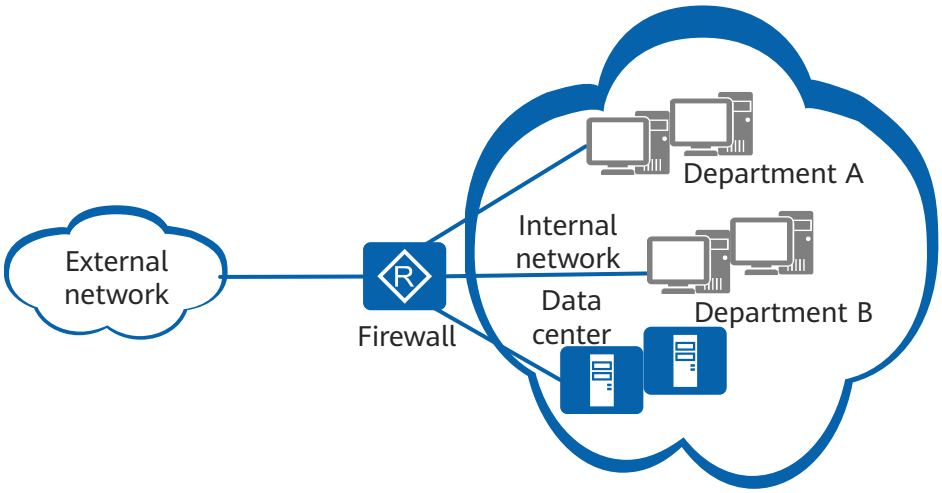
- Data configured by users is not backed up on the master and backup firewalls. Users must perform the same configuration on the master and backup firewalls.
- Firewalls that back up each other must be of the same model, have the same memory, CPU, and configurations.
- Firewalls that back up each other must use the same software version.
- Backup interfaces cannot be service interfaces on the firewall and must be dedicated interfaces. Backup interfaces do not forward data.
- Firewall HSB in the asymmetry route mode is not supported. The bidirectional traffic of a session must pass through the same firewall.
- Statistics data synchronization is not supported. Only TCP/UDP sessions are synchronized.

# 6.3 Application Scenarios for Firewalls

## 6.3.1 Firewall Between the Internal and External Networks

As shown in **Figure 6-20**, a firewall is deployed between the internal and external networks to prevent the external network from attacking the internal network. On an internal network that uses private addresses, the firewall can be used together with NAT and application level gateway (ALG) to improve network security.

**Figure 6-20** Firewall between the internal and external networks

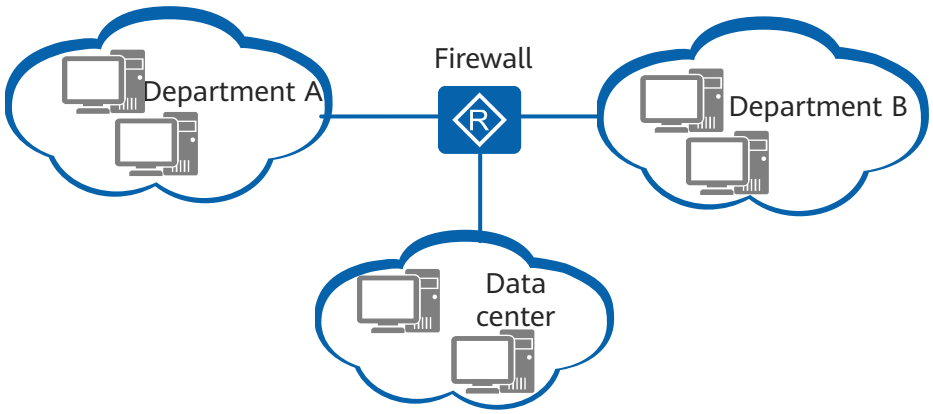



## 6.3.2 Firewall on an Internal Network

As shown in **Figure 6-21**, a firewall is deployed on an internal network to prevent internal attacks and ensure data security. The data center stores important information of a company. Therefore, the firewall must enforce strict policy to protect the data center.


Copyright © Huawei Technologies Co., Ltd.

**Figure 6-21** Firewall on an internal network




# 6.4 Licensing Requirements and Limitations for Firewalls

## Involved Network Elements

Other network elements are not required.

## Licensing Requirements

Firewall is a basic feature of the router and is not under license control.

## Feature Limitations

None

# 6.5 Default Settings for Firewalls

Table 6-1 list the default settings for firewalls.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 6-1** Default settings for firewalls

| Parameter | Default Setting |
| --- | --- |
| Aging time of the firewall session table | The value varies according to the protocol.<br>• DNS: 120 seconds<br>• FTP: 120 seconds<br>• FTP-DATA: 120 seconds<br>• HTTP: 120 seconds<br>• ICMP: 20 seconds<br>• TCP: 600 seconds<br>• TCP-PROXY: 10 seconds<br>• UDP: 120 seconds<br>• SIP: 1800 seconds<br>• SIP-MEDIA: 120 seconds<br>• RTSP: 60 seconds<br>• RTSP-MEDIA: 120 seconds<br>• PPTP: 600 seconds<br>• PPTP-DATA: 600 seconds |
| Default packet filtering mode | Allows outbound packets and denies inbound packets. |
| Maximum session rate for Flood attacks | 1000 pps |
| Maximum length of an ICMP packet | 4000 bytes |
| Maximum session rate for IP address sweeping | 4000 pps |
| Blacklist timeout in IP address sweeping | 20 minutes |
| Maximum session rate for port scanning | 4000 pps |
| Blacklist timeout in port scanning | 20 minutes |
| Thresholds for system traffic statistics and monitoring | The firewall zones support the upper and lower thresholds of protocol packet connections. To view the thresholds, run the **display firewall statistics system** command. |
| Thresholds for zone-based traffic statistics and monitoring | The firewall zones support the upper and lower thresholds of protocol packet connections. To view the thresholds, run the **display firewall statistics zone-ip** command. |


Copyright © Huawei Technologies Co., Ltd.

| Parameter | Default Setting |
| --- | --- |
| Thresholds for IP address-based traffic statistics and monitoring | The firewall zones support the upper and lower thresholds of protocol packet connections. To view the thresholds, run the **display firewall statistics zone-ip** command. |

# 6.6 Configuring Basic Functions of the Firewall

## 6.6.1 Creating a Zone and Adding Interfaces to the Zone

### Context

To configure firewall functions, create zones. Then you can deploy security services according to the priorities of the zones. The device considers that data transmission within a zone is reliable and does not enforce any security policy on intra-zone data transmission. The device verifies data and enforces security policies only when the data is transmitted from one zone to another.

You must configure a priority for a zone before making other configurations. The priority cannot be changed. Each zone must have a different priority. A larger priority value indicates a higher priority.

The firewall takes effect only after interfaces are added to zones.

The device automatically creates a zone named **Local**. The **Local** zone has the highest priority and cannot be deleted. In addition, the priority of this zone cannot be changed, and no interface can be added to this zone. To apply the firewall function to the control packets that need to be processed by the device, use the **Local** zone.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall zone** *zone-name*

A zone is created.

By default, no zone is created on the Router.

**Step 3** Run **priority** *security-priority*

A priority is set for the zone.

**Step 4** Run **quit**

Return to the system view.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 5** Run **interface** *interface-type interface-number*

The interface view is displayed.

**Step 6** Run **zone** *zone-name*

The interface is added to the zone.

Each zone has multiple interfaces, but an interface can be added to only one zone.

**----End**

## 6.6.2 Creating an Interzone

### Context

Any two zones form an interzone. Each interzone has an independent interzone view. Most firewall configurations are performed in the interzone views. After the firewall function is configured, the device checks data transmitted between zones.

In an interzone, data is transmitted in the inbound or outbound direction.

- Inbound: Data flows from a zone with lower priority to a zone with higher priority.
- Outbound: Data flows from a zone with higher priority to a zone with lower priority.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall interzone** *zone-name1 zone-name2*

An interzone is created.

The zones specified for an interzone must have been created on the device.

**----End**

## 6.6.3 Enabling Firewall in an Interzone

### Context

The configured firewall functions take effect only after you enable firewall in an interzone.

To make the firewall function take effect in an interzone that contains the **Local** zone, run the **ip soft-forward enhance enable** command in the system view to enable the enhanced IP forwarding function.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 2** Run **firewall interzone** *zone-name1 zone-name2*

The interzone view is displayed.

The zones *zone-name1* and *zone-name2* must have been created using the **firewall zone** command.

**Step 3** Run **firewall enable**

The firewall is enabled.

By default, the firewall function is disabled in an interzone.

**----End**

# 6.6.4 (Optional) Configuring the Aging Time of the Firewall Session Table

## Context

The Router creates a session table for data flows of each protocol, such as TCP, UDP, and ICMP, to record the connection status of the protocol. An aging time is set for the session table. If a record in the session table does not match any packet within the aging time, the system deletes the record.

To change the aging time for a session of a protocol or a session with a user-defined TCP or UDP port as the destination port, you can configure the aging time of the firewall session table.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall-nat session** { { **dns** | **ftp** | **ftp-data** | **http** | **icmp** | **tcp** | **tcp-proxy** | **udp** | **sip** | **sip-media** | **rtsp** | **rtsp-media** | **pptp** | **pptp-data** } | { **tcp** | **udp** } **user-define** *port-number* } **aging-time** *time-value*

The aging time of the firewall session table is set.

By default, the aging time of each protocol is as follows:

- DNS: 120 seconds
- FTP: 120 seconds
- FTP-data: 120 seconds
- HTTP: 120 seconds
- ICMP: 20 seconds
- TCP: 600 seconds
- TCP-proxy: 10 seconds
- UDP: 120 seconds
- SIP: 1800 seconds
- SIP-media: 120 seconds

 Copyright © Huawei Technologies Co., Ltd. 

- RTSP: 60 seconds
- RTSP-media: 120 seconds
- PPTP: 600 seconds
- PPTP-data: 600 seconds

The default aging time of session entries on a user-defined TCP or UDP port is the same as that of the corresponding protocol.

NOTE

The default aging time is recommended.

**----End**

## 6.6.5 Verifying the Basic Firewall Functions Configuration

### Procedure

- Run the **display firewall zone** [ *zone-name* ] [ **interface** | **priority** ] command to check information about a zone.
- Run the **display firewall interzone** [ *zone-name1 zone-name2* ] command to check information about an interzone.
- Run the **display firewall-nat session aging-time** command to check the aging time of the firewall session table.

**----End**

# 6.7 Configuring the Packet Filtering Firewall

## 6.7.1 (Optional) Configuring the Default Processing Mode for Unmatched Packets

### Context

By default, a firewall allows all the outbound packets and denies all the inbound packets.

If an ACL is applied to the inbound or outbound packets in an interzone, the firewall filters packets according to the ACL rules. If packets do not match the ACL, the firewall uses the default processing mode for the packets.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall interzone** *zone-name1 zone-name2*

The interzone view is displayed.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 3** Run **packet-filter default** { **deny** | **permit** } { **inbound** | **outbound** }

The default processing mode for unmatched packets is configured.

NOTE

When you are modifying filtering rules in an interzone, some sessions may not be filtered properly according to the rules. Therefore, after the modification is complete, use the **reset firewall session** command to delete all existing firewall session entries.

**----End**

# 6.7.2 Configuring ACL-based Packet Filtering in an Interzone

## Context

When data is transmitted between two zones, the ACL-based packet filtering firewall enforces the packet filtering policies according to the ACL rules.

NOTE

If a tunnel is set up on a physical interface, the traffic destined for or from the tunnel is sent or received by the tunnel interface. If you need to configure the firewall function, configure the zone on the tunnel interface, but not on the physical interface. Otherwise, the firewall function cannot take effect.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **acl** [ **number** ] *acl-number* [ **match-order** { **config** | **auto** }]

Or **acl ipv6** [ **number** ] *acl6-number*

An ACL or ACL6 is created, and the ACL view or ACL6 view is displayed.

NOTE

The ACLs for filtering packets include basic ACLs and advanced ACLs.

The ACL6-based packet filtering can use basic ACL6 and advanced ACL6.

**Step 3** Run **rule** (basic ACL view), **rule** (advanced ACL view), **rule** (basic ACL6 view), or **rule** (advanced ACL6 view)

An ACL rule is configured.

NOTICE

If **destination pd** *destination-dhcpv6-prefix* or **source pd** *source-dhcpv6-prefix* is specified in the **rule (advanced ACL6 view)** command, when the IPv6 address prefix obtained from the DHCPv6 server changes, update the session table on the firewall so that the new IPv6 address prefix can take effect. During the update, service forwarding on the firewall may be temporarily affected. After the update, services automatically recover.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

When the ACL6-based packet filtering firewall function is configured, the **fragment** parameter is not supported in an ACL6 rule.

**Step 4** Run **quit**

Return to the system view.

**Step 5** Run **firewall interzone** *zone-name1 zone-name2*

The interzone view is displayed.

**Step 6** Run **packet-filter** { *acl-number* | **default** { **deny** | **permit** } } { **inbound** | **outbound** }or **packet-filter ipv6** *acl6-number* { **inbound** | **outbound** }

The ACL-based packet filtering or ACL6 packet filtering is configured.

You can configure ACL-based packet filtering in the interzone for inbound or outbound packets.

1. When **permit** is used in the ACL rule:
   - When the ACL is applied to the **inbound** traffic, the system forwards the packets matching the ACL rule sent from the low-priority zone to the high-priority zone.
   - When the ACL is applied to the **outbound** traffic, the system forwards the packets matching the ACL rule sent from the high-priority zone to the low-priority zone.
2. When **deny** is used in the ACL rule:
   - When the ACL is applied to the **inbound** traffic, the system discards the packets matching the ACL rule sent from the low-priority zone to the high-priority zone.
   - When the ACL is applied to the **outbound** traffic, the system discards the packets matching the ACL rule sent from the high-priority zone to the low-priority zone.
3. When an ACL does not contain rules:
   - When the ACL is applied to the **inbound** traffic, the ACL does not take effect, and the system discards all packets sent from the low-priority zone to the high-priority zone.
   - When the ACL is applied to the **outbound** traffic, the ACL does not take effect, and the system discards all packets sent from the high-priority zone to the low-priority zone.

You can configure ACL6-based packet filtering in the outbound and inbound directions of an interzone.

When the ACL6 does not contain rules:

- When the ACL6 is applied to the **inbound** traffic, the ACL6 does not take effect, and the system discards all packets sent from the low-priority zone to the high-priority zone.
- When the ACL6 is applied to the **outbound** traffic, the ACL6 does not take effect, and the system discards all packets sent from the high-priority zone to the low-priority zone.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 7** (Optional) Run **bypass** [ **session-overrun** ]

The packet filtering firewall bypass function is enabled in an interzone.

By default, the packet filtering firewall bypass function is disabled in an interzone.

**----End**

## 6.7.3 Verifying the Packet Filtering Firewall Configuration

### Procedure

- Run the **display firewall interzone** [ *zone-name1 zone-name2* ] command to check information about packet filtering.
- Run the **display acl** *acl-number* command to check the ACL configuration.

**----End**

# 6.8 Configuring Stateful Firewall (ASPF)

### Context

Application specific packet filter (ASPF) is status-based packet filtering. ASPF detects the application-layer sessions that attempt to pass the firewall, and discards undesired packets. ASPF can detect and filter FTP, SIP, and RTSP packets at the application layer.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall interzone** *zone-name1 zone-name2*

The interzone view is displayed.

**Step 3** Run **detect aspf** { **ftp** | **rtsp** | **sip** }

ASPF is configured.

Generally, application-layer protocol packets are transmitted bidirectionally, so the direction does not need to be specified. The firewall automatically checks the packets in both directions.

By default, ASPF is not configured in an interzone.

**----End**

### Verifying the Configuration

- Run the **display firewall interzone** [ *zone-name1 zone-name2* ] command to check ASPF information in the interzone.

 Copyright © Huawei Technologies Co., Ltd. 

# 6.9 Configuring the Blacklist

## 6.9.1 Enabling the Blacklist Function

### Context

A blacklist filters packets based on source IP addresses. Compared with ACLs, the blacklist uses simpler matching fields and therefore filters packets at a higher speed. Packets from certain IP addresses can be filtered out.

The firewall can dynamically add IP addresses to the blacklist. When detecting an attack from an IP address, the firewall adds the IP address to the blacklist to filter out all packets from this IP address. To enable the firewall to dynamically create blacklist entries, enable IP address scanning attack defense and port scanning attack defense.

Entries can be added to the blacklist manually or dynamically. After IP address scanning and port scanning defense is enabled on the attack defense module, the firewall can dynamically create blacklist entries. When the connection rate of an IP address or a port exceeds the threshold, the firewall considers that a scanning attack occurs and adds the source IP address to the blacklist. All the packets from this source IP address are then filtered out.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** (Optional) Run **firewall defend ip-sweep enable**

The IP address sweeping attack defense is enabled.

**Step 3** (Optional) Run **firewall defend ip-sweep** { **blacklist-expire-time** *interval* | **max-rate** *rate-value* }

The parameters for IP address sweeping attack defense are set.

**Step 4** (Optional) Run **firewall defend port-scan enable**

The port scanning attack defense is enabled.

**Step 5** (Optional) Run **firewall defend port-scan** { **blacklist-expire-time** *interval* | **max-rate** *rate-value* }

The parameters for port scanning attack defense are set.

For scanning attack defense, the following two parameters need to be set:

- Maximum session rate: When the session rate of an IP address or a port exceeds the limit, the firewall considers that a scanning attack occurs. Then the firewall adds the IP address or port to the blacklist to reject new sessions from the IP address or port.

 Copyright © Huawei Technologies Co., Ltd. 

- Blacklist timeout: After an IP address or a port stays in the blacklist for a specified period, it is deleted from the blacklist. Then new connections can be initiated from this IP address or port.

By default, the maximum session rate for IP address sweeping and port scanning attack defense is 4000 pps, and the blacklist timeout is 20 minutes.

**Step 6** Run **firewall blacklist enable**

The blacklist function is enabled.

By default, the blacklist function is disabled.

**----End**

## 6.9.2 Configuring a Blacklist Entry

### Context

After an IP address is added to the blacklist, the firewall denies packets from this IP address until this entry expires.

When adding an entry to the blacklist, you can specify the IP address, aging time, and VPN instance. The aging time refers to the amount of time the IP address is effective in the blacklist. When the aging time expires, the IP address is released from the blacklist. If the aging time is not specified, the IP address is always valid in the blacklist.

An IP address can be added to the blacklist regardless of whether the blacklist is enabled or not. You can add entries to the blacklist when the blacklist is disabled, but the entries do not take effect until the blacklist is enabled.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall blacklist** *ip-address* [ **vpn-instance** *vpn-instance-name* ] [ **expire-time** *minutes* ]

An entry is added to the blacklist.

NOTE

The blacklist entries without an aging time are saved in the configuration file. The entries configured with an aging time are not saved in to the configuration file, but you can view them by using the **display firewall blacklist** command.

**Step 3** (Optional) Run **firewall black-white-list save configuration-file** *configuration-file-name*

The blacklist and whitelist are saved to the specified configuration file. You can use the blacklist and whitelist later by loading this configuration file.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

# 6.9.3 Configuring Blacklist or Whitelist Entries in Batches

## Context

You can configure blacklist and whitelist entries in a batch by loading a configuration file. The configuration file for storing the blacklist and whitelist must be available.

The entries in the whitelist take effect immediately, and you do not need to enable the whitelist function.

The configuration file must be in txt format and contain the following fields:

```
[FirewallBlacklist]      # A blacklist entry
IPAddress =              # An IP address in the blacklist, in dotted decimal notation
VPNName =                  # (Optional) VPN instance of the blacklist entry
[FirewallWhitelist]      # A whitelist entry
IPAddress =              # An IP address in the whitelist, in dotted decimal notation
VPNName =                  # (Optional) VPN instance of the whitelist entry
```

A configuration file can contain multiple entries, but each entry must be edited separately. Blank lines are allowed between lines.

```
[FirewallBlacklist]
IPAddress = 10.10.10.1
VPNName = vpna
[FirewallBlacklist]
IPAddress = 10.10.10.2
VPNName =

[FirewallWhitelist]
IPAddress = 10.10.10.3
VPNName = vpnb
[FirewallWhitelist]
IPAddress = 10.20.20.1
VPNName =
```

**NOTE**

A configuration file can contain up to 50000 lines.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall black-white-list load configuration-file** *configuration-file-name*

A blacklist and whitelist configuration file is loaded.

**Step 3** Run **firewall blacklist enable**

The blacklist function is enabled.

**Step 4** (Optional) Run **firewall black-white-list save configuration-file** *configuration-file-name*

The blacklist and whitelist are saved to the specified configuration file.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## 6.9.4 Verifying the Blacklist Configuration

### Procedure

- Run the **display firewall blacklist** { **all** | *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **dynamic** | **static** | **vpn-instance** *vpn-instance-name* } command to check information about the blacklist.
- Run the **display firewall blacklist configuration** command to check the status of the blacklist function.

**----End**

# 6.10 Configuring the Whitelist

## 6.10.1 Configuring a Whitelist Entry

### Context

The whitelist prevents specified IP addresses from being added to the blacklist. The IP addresses in the whitelist will not be added to the blacklist statically or dynamically. An entry in the whitelist is identified by a source VPN and a source IP address.

You can specify the IP address, aging time, and VPN instance when adding an entry to the whitelist. The aging time refers to amount of time the IP address is effective in the whitelist. When the aging time expires, the IP address is released from the whitelist. If the aging time is not specified, the IP address is always valid in the whitelist.

Entries in the whitelist take effect directly and you do not need to enable the whitelist function.

The whitelist is applicable to networks where packets sent from some devices are valid service packets similar to IP address sweeping or port scanning attack packets. The whitelist prevents these devices from being added to the blacklist.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall whitelist** *ip-address* [ **vpn-instance** *vpn-instance-name* ] [ **expire-time** *minutes* ]

An entry is added to the whitelist.

**Step 3** (Optional) Run **firewall black-white-list save configuration-file** *configuration-file-name*

The blacklist and whitelist are saved to the specified configuration file. You can use the blacklist and whitelist later by loading this configuration file.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

# 6.10.2 Configuring Blacklist or Whitelist Entries in Batches

## Context

You can configure blacklist and whitelist entries in a batch by loading a configuration file. The configuration file for storing the blacklist and whitelist must be available.

The entries in the whitelist take effect immediately, and you do not need to enable the whitelist function.

The configuration file must be in txt format and contain the following fields:

```
[FirewallBlacklist]      # A blacklist entry
IPAddress =              # An IP address in the blacklist, in dotted decimal notation
VPNName =                  # (Optional) VPN instance of the blacklist entry
[FirewallWhitelist]      # A whitelist entry
IPAddress =              # An IP address in the whitelist, in dotted decimal notation
VPNName =                  # (Optional) VPN instance of the whitelist entry
```

A configuration file can contain multiple entries, but each entry must be edited separately. Blank lines are allowed between lines.

```
[FirewallBlacklist]
IPAddress = 10.10.10.1
VPNName = vpna
[FirewallBlacklist]
IPAddress = 10.10.10.2
VPNName =

[FirewallWhitelist]
IPAddress = 10.10.10.3
VPNName = vpnb
[FirewallWhitelist]
IPAddress = 10.20.20.1
VPNName =
```

**NOTE**

A configuration file can contain up to 50000 lines.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall black-white-list load configuration-file** *configuration-file-name*

A blacklist and whitelist configuration file is loaded.

**Step 3** Run **firewall blacklist enable**

The blacklist function is enabled.

**Step 4** (Optional) Run **firewall black-white-list save configuration-file** *configuration-file-name*

The blacklist and whitelist are saved to the specified configuration file.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## 6.10.3 Verifying the Whitelist Configuration

### Procedure

- Run the **display firewall whitelist** { **all** | *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **vpn-instance** *vpn-instance-name* } command to check information about the whitelist.
- Run the **display firewall blacklist** { { **all** | *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **dynamic** | **static** | **vpn-instance** *vpn-instance-name* } command to check information about the blacklist.

**----End**

# 6.11 Configuring Port Mapping

### Context

Application-layer protocols use well-known ports for communication. Port mapping enables you to define new port numbers for application-layer protocols, such as FTP, DNS, HTTP, SIP, PPTP and RTSP, which protect servers against service-specific attacks. Port mapping applies to service-sensitive features such as application specific packet filter (ASPF) and Network Address Translation (NAT).

Port mapping is implemented based on basic ACLs (2000 to 2999). The firewall matches destination IP addresses of packets with the IP addresses configured in basic ACL rules and performs port mapping only for the packets matching the ACL rules.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **port-mapping** { **dns** | **ftp** | **http** | **sip** | **rtsp** | **pptp** } **port** *port-number* **acl** *acl-number*

Port mapping is configured.

You can map multiple ports to a protocol, or map a port to multiple protocols. The mappings, however, must be distinguished by ACLs. That is, packets matching different ACL rules use different mapping entries.

NOTE

Port mapping identifies the protocol type of the packets destined for an IP address (such as the IP address of a WWW server). Therefore, when configuring the basic ACL rules, match the destination IP addresses of the packets with the source IP addresses defined in ACL rules.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

### Verifying the Configuration

- Run the **display port-mapping** [ **dns** | **ftp** | **http** | **rtsp** | **sip** | **port** *port-number* | **pptp** ] command to check information about port mapping.

# 6.12 Configuring Attack Defense

## 6.12.1 Enabling the Attack Defense Function

### Context

The attack defense function protects the CPU of a server against attacks to ensure that the server operates normally when it is attacked. You can enable different types of attack defense as required.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Enable attack defense.

- Run **firewall defend all enable**
  All the attack defense functions are enabled.
- Run **firewall defend fraggle enable**
  The Fraggle attack defense is enabled.
- Run **firewall defend icmp-flood enable**
  The ICMP Flood attack defense is enabled.
- Run **firewall defend icmp-redirect enable**
  The ICMP Redirect attack defense is enabled.
- Run **firewall defend icmp-unreachable enable**
  The ICMP Unreachable attack defense is enabled.
- Run **firewall defend ip-fragment enable**
  The IP-Fragment attack defense is enabled.
- Run **firewall defend ip-sweep enable**
  The IP address sweeping attack defense is enabled.
- Run **firewall defend land enable**
  The Land attack defense is enabled.
- Run **firewall defend large-icmp enable**
  The large ICMP packet attack defense is enabled.
- Run **firewall defend ping-of-death enable**
  The Ping of Death attack defense is enabled.
- Run **firewall defend port-scan enable**
  The port scanning attack defense is enabled.

 Copyright © Huawei Technologies Co., Ltd. 

- Run **firewall defend smurf enable**
  The Smurf attack defense is enabled.
- Run **firewall defend syn-flood enable**
  The SYN Flood attack defense is enabled.
- Run **firewall defend tcp-flag enable**
  The TCP flag attack defense is enabled.
- Run **firewall defend teardrop enable**
  The Teardrop attack defense is enabled.
- Run **firewall defend tracert enable**
  The Tracert attack defense is enabled.
- Run **firewall defend udp-flood enable**
  The UDP Flood attack defense is enabled.
- Run **firewall defend winnuke enable**
  The WinNuke attack defense is enabled.

By default, no attack defense function is enabled.

**----End**

## 6.12.2 Setting the Parameters for Flood Attack Defense

### Context

When configuring Flood attack defense, specify the zones or IP addresses to be protected; otherwise, the attack defense parameters are invalid. You can also specify the maximum session rate. When the session rate exceeds the limit, the firewall considers that an attack occurs and takes measures.

Flood attack defense parameters configured for an IP address take precedence over those configured for a zone. If Flood attack defense is configured for both a specified IP address and the zone where the IP address resides, the configuration for the IP address takes effect. If you delete the attack defense configuration for the IP address, the attack defense configuration for the zone takes effect.

Steps 2-4 are optional and can be performed in any sequence. You can perform any of these steps as required.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall defend icmp-flood** { **ip** *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **zone** *zone-name* } [ **max-rate** *rate-value* ]

The parameters for ICMP Flood attack defense are set.

By default, the maximum session rate for Flood attacks is 1000 pps.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 3** Run **firewall defend syn-flood** { **ip** *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **zone** *zone-name* } [ **max-rate** *rate-value* ] [ **tcp-proxy** { **auto** | **off** | **on** } ]

The parameters for SYN Flood attack defense are set.

By default, the maximum session rate for Flood attacks is 1000 pps.

**Step 4** Run **firewall defend udp-flood** { **ip** *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **zone** *zone-name* } [ **max-rate** *rate-value* ]

The parameters for UDP Flood attack defense are set.

By default, the maximum session rate for Flood attacks is 1000 pps.

**----End**

## 6.12.3 Configuring Large ICMP Packet Attack Defense

### Context

For large ICMP packet attack defense, you only need set the maximum packet length. When the length of an ICMP packet exceeds the limit, the firewall considers the packet as an attack packet and discards it.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall defend large-icmp max-length** *length*

The maximum length of ICMP packet is set.

By default, the maximum length of an ICMP packet is 4000 bytes.

**----End**

## 6.12.4 Setting Parameters for Scanning Attack Defense

### Context

For scanning attack defense, the following two parameters need to be set:

- Maximum session rate: When an IP address accesses another IP address or port at a rate higher than this value, the firewall considers that a scanning attack occurs. Then the firewall adds the IP address or port to the blacklist to reject new sessions from the IP address or port.
- Blacklist timeout: After an IP address or port stays in the blacklist for a specified period, the firewall deletes the IP address or port from the blacklist and allows new sessions from the IP address or port.

Step 2 and step 3 are optional and can be performed in any sequence. You can perform the steps as required.

 Copyright © Huawei Technologies Co., Ltd. 

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall defend ip-sweep** { **blacklist-expire-time** *interval* | **max-rate** *rate-value* }

The parameters for IP address sweeping attack defense are set.

**Step 3** Run **firewall defend port-scan** { **blacklist-expire-time** *interval* | **max-rate** *rate-value* }

The parameters for port scanning attack defense are set.

By default, the maximum session rate for IP address sweeping and port scanning attack defense is 4000 pps, and the blacklist timeout is 20 minutes.

**----End**

## 6.12.5 Verifying the Attack Defense Configuration

### Procedure

- Run the **display firewall defend** { **flag** | { **icmp-flood** | **syn-flood** | **udp-flood** } [ **ip** [ *ip-address* [ **vpn-instance** *vpn-instance-name* ] ] | **zone** [ *zone-name* ] ] | *other-attack-type* } command to check information about attack defense.

**----End**

# 6.13 Configuring Traffic Statistics and Monitoring

### Context

The Router supports traffic statistics and monitoring at the system level, zone level, and IP address level.

## 6.13.1 Setting the Session Thresholds for System-Level Traffic Statistics and Monitoring

### Context

System-level traffic statistics and monitoring take effect on all the data flows in interzones that are enabled with the firewall feature. That is, the Router collects statistics about the ICMP, TCP, and UDP sessions in the interzones. When the number of sessions exceeds the threshold, the Router restricts the sessions until the number of sessions is less than the threshold.

### Procedure

**Step 1** Run **system-view**

 Copyright © Huawei Technologies Co., Ltd. 

The system view is displayed.

**Step 2** Run **firewall statistics system enable**

The system-level traffic statistics and monitoring are enabled.

By default, the system-level traffic statistics and monitoring is disabled.

**Step 3** (Optional) Run **firewall statistics system connect-number** { **frag** | **icmp** | **tcp** | **tcp-proxy** | **udp** } **high** *high-threshold* **low** *low-threshold*

The session thresholds for the system-level traffic statistics and monitoring are set.

For the system-level traffic statistics, you can set the thresholds for each type of session. For example, you can set the upper threshold for TCP sessions to 15000 and lower threshold to 12000. When the number of TCP sessions in all interzones exceeds 15000, the Router denies all new TCP sessions in the interzone and reports an alarm to the information center. If the number of TCP sessions falls below 12,000, a new TCP session can be established, a traffic recovery log is generated, and the log is output to the information center.

**----End**

## 6.13.2 Setting the Session Thresholds for Zone-Level Traffic Statistics and Monitoring

### Context

The zone-level traffic statistics and monitoring take effect on the data flows between zones. That is, the Router counts the total number of TCP and UDP sessions between the local zone and other zones. When the number of connections between the local zone and all the other zones or the number of connections in a certain direction exceeds the threshold, the Router forbids new sessions until the number of sessions is smaller than the threshold.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall zone** *zone-name*

The zone view is displayed.

**Step 3** Run **statistics zone enable** { **inzone** | **outzone** }

The zone-level traffic statistics and monitoring are enabled.

By default, the zone-level traffic statistics and monitoring is disabled.

**Step 4** (Optional) Run **statistics connect-number zone** { **inzone** | **outzone** } { **icmp** | **tcp** | **udp** } **high** *high-threshold* **low** *low-threshold*

The session thresholds for the zone-level traffic statistics and monitoring are set.

You can set the thresholds for ICMP, TCP, and UDP sessions in the inbound and outbound directions respectively. For example, you can set the upper and lower

 Copyright © Huawei Technologies Co., Ltd. 

thresholds for TCP sessions in the inbound direction to 15000 and 13000, respectively. When the number of TCP sessions initiated by this zone exceeds 15000, the device denies new TCP sessions from this zone. Only when the number of TCP sessions initiated by this zone falls below 13000, the device permits new TCP sessions from this zone.

**----End**

## 6.13.3 Setting the Session Thresholds for IP Address-Level Traffic Statistics and Monitoring

### Context

The IP address-level traffic statistics and monitoring counts and monitors the TCP and UDP sessions set up on an IP address in a zone. The Router determines whether to restrict the connections in a certain direction by checking whether the number of the TCP or UDP connection requests sent from a source IP address (or received by a destination address) exceeds the threshold. This function prevents DoS caused by the malicious attack or busy systems.

When the number of TCP and UDP sessions falls below the threshold, the source IP address can initiate sessions and the destination address can receive sessions.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall zone** *zone-name*

The zone view is displayed.

**Step 3** Run **statistics ip enable** { **inzone** | **outzone** }

The IP address-level traffic statistics and monitoring are enabled.

By default, the IP address-level traffic statistics and monitoring is disabled.

**Step 4** (Optional) Run **statistics connect-number ip** [ **range** *beginip endip* ] { **inzone** | **outzone** } { **icmp** | **tcp** | **udp** } **high** *high-threshold* **low** *low-threshold*

The session thresholds for the IP address-level traffic statistics and monitoring are set.

The thresholds for ICMP, TCP, and UDP sessions can be set in the inbound and outbound directions respectively. For example, when the upper threshold for the number of TCP sessions in the inbound direction is 10,000 and the lower threshold is 8,000, and the number of TCP sessions initiated by the local area to other areas exceeds 10,000, the device rejects the new TCP session request initiated from the local area. When the total number of TCP sessions initiated by the local area to other areas decreases to 8,000, the local area can initiate new TCP session requests to other areas.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## 6.13.4 Verifying the Traffic Statistics and Monitoring Configuration

### Procedure

- Run the **display firewall statistics system** command to check information about system-level traffic statistics and monitoring.
- Run the **display firewall statistics zone** *zone-name* { **inzone** | **outzone** } **all** command to check information about zone-level traffic statistics and monitoring.
- Run the **display firewall statistics zone-ip** *zone-name* command to check information about IP address-level traffic statistics and monitoring.

**----End**

# 6.14 Configuring the Firewall Log Function

### Context

Firewall logs include session logs, statistics logs, attack defense logs, packet filtering logs and blacklist logs.

The session logs are exported to a log host in real time; therefore, you need to configure the log host first. To configure the log host, configure the IP address and port number of the log host as well as the source IP address and source port number that the Router uses to communicate with the log host.

An ACL is referenced in the interzone view to determine the sessions to be recorded in the logs. The ACLs can be configured for incoming and outgoing traffic.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall log binary-log host** *host-ip-address host-port* **source** *source-ip-address source-port* [ **vpn-instance** *vpn-instance-name* ]

A session log host is configured.

By default, no session log host is configured.

**Step 3** Run **firewall log** { **all** | **blacklist** | **defend** | **session** | **statistics** | **packet-filter** } **enable**

The log function is enabled on the firewall.

By default, the log function is disabled on a firewall.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

To improve configuration efficiency, run the **firewall log all enable** command to enable the firewall log function. After the command is executed, the traffic statistics, attack, and blacklist log functions take effect on the firewall. To enable the packet filtering log function, you also need to perform **Configuring packet filtering log in the interzone**; to enable the flow log function, you also need to perform **Configuring flow log in the interzone**.

- Configuring packet filtering log in the interzone
  a. Run **firewall interzone** *zone-name1 zone-name2*
     The interzone view is displayed.
  b. Run **packet-filter logging** [ { **inbound** | **outbound** } [ **permit** | **deny** ] ]
     The packet filtering log is enabled in the interzone.
     By default, the packet filtering log is disabled in the interzone.
  c. Run **quit**
     Return to the system view.
- Configuring flow log in the interzone
  a. Run **firewall interzone** *zone-name1 zone-name2*
     The interzone view is displayed.
  b. Run **session-log** *acl-number* { **inbound** | **outbound** }
     The conditions of recording flow logs are configured.
     By default, no condition is configured in an interzone for recording flow logs.
  c. Run **quit**
     Return to the system view.

**Step 4** (Optional) Run **firewall log** { **blacklist** | **defend** | **session** | **statistics packet-filter** } **log-interval** *time*

The interval for exporting logs is set.

By default, logs are exported every 30 seconds.

**----End**

### Verifying the Configuration

- Run the **display firewall log configuration** command to check logs on the firewall.

# 6.15 Configuring Virtual Firewalls

## 6.15.1 Configuring a VPN Instance to Identify a Virtual Firewall

### Context

You can configure VPN instances to identify virtual firewalls. A VPN instance corresponds to a virtual firewall. Before configuring a virtual firewall, create a VPN

 Copyright © Huawei Technologies Co., Ltd. 

instance and bind interfaces to the VPN instance. The interfaces bound to a VPN instance belong to the same firewall and can be configured with independent security policies.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **ip vpn-instance** *vpn-instance-name*

A VPN instance is created, and the VPN instance view is displayed.

**Step 3** (Optional) Run **description** *description-information*

The description of the VPN instance is configured.

**Step 4** Run **route-distinguisher** *route-distinguisher*

The RD of the VPN instance is configured.

After a VPN instance is created, you must specify the RD for the VPN instance. Otherwise, you cannot perform subsequent operations.

**Step 5** Run **interface** *interface-type interface-number*

The interface view is displayed.

**Step 6** Run **ip binding vpn-instance** *vpn-instance-name*

The interface is bound to the VPN instance.

Bind the interface to the VPN instance before configuring an IP address for the interface. If the interface IP address is configured before the interface is bound to the VPN instance, the interface IP address is deleted. You need to reconfigure the IP address for the interface.

**Step 7** Run **ip address** *ip-address* { *mask* | *mask-length* }

An IP address is configured for the interface.

**----End**

# 6.15.2 Configuring Security Functions for a Virtual Firewall

## Context

The procedure for configuring security functions on a virtual firewall is similar to the procedure for configuring security functions on a firewall. You must configure security functions on each virtual firewall independently to meet different service requirements. You can configure the following security functions:

- Packet filtering firewall
- ASPF
- Port mapping
- Aging time of the firewall session table

 Copyright © Huawei Technologies Co., Ltd. 

- Attack defense

When configuring the following functions on a virtual firewall, you must specify a VPN instance:

- **Configuring a blacklist on the virtual firewall**
- **Configuring a whitelist on the virtual firewall**
- **Configuring defense against ICMP Flood attacks**
- **Configuring defense against SYN Flood attacks**
- **Configuring defense against UDP Flood attacks**

## Procedure

- Configuring a blacklist on the virtual firewall
  a. Run **system-view**

     The system view is displayed.
  b. Run **firewall blacklist enable**

     The blacklist function is enabled.
  c. Run **firewall blacklist** *ip-address* [ **vpn-instance** *vpn-instance-name* ] [ **expire-time** *minutes* ]

     An entry is added to the blacklist.
- Configuring a whitelist on the virtual firewall
  a. Run **system-view**

     The system view is displayed.
  b. Run **firewall whitelist** *ip-address* [ **vpn-instance** *vpn-instance-name* ] [ **expire-time** *minutes* ]

     An entry is added to the whitelist.
- Configuring defense against ICMP Flood attacks
  a. Run **system-view**

     The system view is displayed.
  b. Run **firewall defend icmp-flood enable**

     The ICMP Flood attack defense function is enabled.
  c. Run **firewall defend icmp-flood** { **ip** *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **zone** *zone-name* } [ **max-rate** *rate-value* ]

     The parameters of ICMP Flood attack defense are set.
- Configuring defense against SYN Flood attacks
  a. Run **system-view**

     The system view is displayed.
  b. Run **firewall defend syn-flood enable**

     The SYN Flood attack defense function is enabled.
  c. Run **firewall defend syn-flood** { **ip** *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **zone** *zone-name* } [ **max-rate** *rate-value* ] [ **tcp-proxy** { **auto** | **off** | **on** } ]

 Copyright © Huawei Technologies Co., Ltd. 

The parameters of SYN Flood attack defense are set.

- Configuring defense against UDP Flood attacks
  a. Run **system-view**

     The system view is displayed.
  b. Run **firewall defend udp-flood enable**

     The UDP Flood attack defense function is enabled.
  c. Run **firewall defend udp-flood** { **ip** *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **zone** *zone-name* } [ **max-rate** *rate-value* ]

     The parameters of UDP Flood attack defense are set.

**----End**

## 6.15.3 Verifying the Virtual Firewall Configuration

### Procedure

- Run the **display firewall zone** [ *zone-name* ] [ **interface** | **priority** ] command to check information about a zone.
- Run the **display firewall interzone** [ *zone-name1 zone-name2* ] command to check information about an interzone.
- Run the **display firewall blacklist** { **all** | *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **dynamic** | **static** | **vpn-instance** *vpn-instance-name* } command to check information about the blacklist.
- Run the **display firewall whitelist** { **all** | *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **vpn-instance** *vpn-instance-name* } command to check information about the whitelist.
- Run the **display firewall defend** { **flag** | { **icmp-flood** | **syn-flood** | **udp-flood** } [ **ip** [ *ip-address* [ **vpn-instance** *vpn-instance-name* ] ] | **zone** [ *zone-name* ] ] | *other-attack-type* } command to check information about attack defense.

**----End**

# 6.16 Configuring Firewalls in HSB Mode

## 6.16.1 Configuring an HSB Service

### Context

An HSB service establishes an HSB channel for transmitting packets of other services and maintains the link status by notifying the HSB group of the faulty link.

An HSB service provides the following functions:

- Establishing an HSB channel: A TCP channel is established for sending HSB packets by setting the IP addresses and port numbers of the local and peer

 Copyright © Huawei Technologies Co., Ltd. 

devices. The HSB service provides packet sending and receiving for other services and notifies link status changes.

- Maintaining the link status of the HSB channel: HSB packets are sent and retransmitted to prevent long TCP interruption that is not detected by the protocol stack. If a device does not receive an HSB packet from the peer device within the period (retransmission interval x retransmission times), the local device receives a message indicating the exception and then re-establishes a channel to the peer.

NOTE

- Parameters for the HSB channel must be configured on the local and remote ends at the same time. The source IP address, destination IP address, source port, and destination port of the local end are the destination IP address, source IP address, destination port, and source port of the remote end, respectively.
- Parameters of HSB service packets, including the interval and packet retransmission times, must be the same on both ends.
- Pay attention to the following points when configuring a shared key:
  - Configuring a shared key for HSB service is not recommended in a secure network environment because this configuration will degrade the HSB performance. If the shared key is required, ensure that the same shared key is configured at both ends of the HSB service. Inconsistent keys on both ends will cause frequent interruption of the HSB channel.
  - The **key** command must be configured before the **service-ip-port** command; otherwise, the **key** command will fail to be configured.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **hsb-service** *service-index*

An HSB service is created and the HSB service view is displayed.

By default, no HSB service is created.

**Step 3** (Optional) Run **key cipher** *key-string*

The key used by the HSB devices is configured.

By default, the key used by HSB devices is not configured.

**Step 4** Run **service-ip-port local-ip** *local-ip-address* **peer-ip** *peer-ip-address* **local-data-port** *local-port* **peer-data-port** *peer-port*

The IP address and port number of an HSB channel is configured.

By default, the IP address and port number of an HSB channel are not configured.

**Step 5** (Optional) Run **service-keep-alive detect retransmit** *retransmit-times* **interval** *interval-value*

The retransmission times and interval of HSB packets are set.

The default number of retransmission times is 5, and the default retransmission interval is 3 seconds.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

# 6.16.2 Configuring an HSB Group

## Context

An HSB group instructs service modules to perform batch backup, real-time backup, and status synchronization. The backup of services depends on the status negotiation and event notification mechanisms provided by the HSB group, synchronizing services on the master and backup devices.

An HSB group synchronizes backup information and responds to link status changes through the HSB channel established by the HSB service. To make the HSB group work properly, bind an HSB service to the HSB group. In addition, the HSB group must be bound to a VRRP group to negotiate the service status based on the VRRP status. By monitoring the changes in the bound HSB channel status and VRRP status, the HSB group instructs service modules to perform batch backup, real-time backup, and status synchronization.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **hsb-group** *group-index*

An HSB group is created and the HSB group view is displayed.

By default, no HSB group is created.

**Step 3** Run **bind-service** *service-index*

An HSB service is configured for binding to the HSB group.

By default, no HSB service is bound to an HSB group.

**Step 4** Run **track vrrp vrid** *virtual-router-id* **interface** *interface-type interface-number*

A VRRP group is configured for binding to the HSB group.

By default, no HSB group is bound to a VRRP group.

**Step 5** Run **quit**

The system view is displayed.

**Step 6** (Optional) Run **hsb-service-type firewall hsb-group** *group-index*

The firewall service is bound to the HSB group

NOTE

STP, VRRP, and MTU cannot be configured on the HSB link.

Bind firewall service to an HSB group before enabling the HSB group.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## 6.16.3 Enabling an HSB Group

### Context

An HSB group takes effect and notifies the service modules of status changes only after the HSB group is enabled.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **hsb-group** *group-index*

The HSB group view is displayed.

**Step 3** Run **hsb enable**

The HSB group is enabled.

**----End**

## 6.16.4 Verifying the HSB Configuration

### Procedure

- Run the **display hsb-group** *group-index* command to view information about the HSB group.
- Run the **display hsb-service** *service-index* command to view information about the HSB service.

**----End**

# 6.17 Maintaining the Firewall

## 6.17.1 Displaying the Firewall Configuration

### Procedure

- Run the **display firewall zone** [ *zone-name* ] [ **interface** | **priority** ] command to view the configurations of all zones or a specified zone.
- Run the **display firewall interzone** [ *zone-name1 zone-name2* ] command to view the configurations of an interzone.
- Run the **display firewall blacklist configuration** command to view the status of the blacklist function.
- Run the **display firewall blacklist** { **all** | *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **dynamic** | **static** | **vpn-instance** *vpn-instance-name* } command to view the blacklist entries.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **display firewall whitelist** { **all** | *ip-address* [ **vpn-instance** *vpn-instance-name* ] | **vpn-instance** *vpn-instance-name* } command to view the whitelist entries.
- Run the **display firewall statistics system** [ **normal all** | **defend** ] command to view the system-level traffic statistics.
- Run the **display firewall statistics zone** *zone-name* { **inzone** | **outzone** } **all** command to view the zone-level traffic statistics and traffic monitoring information.
- Run the **display firewall statistics zone-ip** *zone-name* command to view the status of traffic monitoring function and session thresholds for each protocol.
- Run the **display firewall-nat session aging-time** command to view the timeout of entries in the session table.
- Run the **display port-mapping** [ **dns** | **ftp** | **http** | **rtsp** | **sip** | **port** *port-number* | **pptp** ] command to view the mappings between application-layer protocols and ports.
- Run the **display firewall defend** { **flag** | { **icmp-flood** | **syn-flood** | **udp-flood** } [ **ip** [ *ip-address* [ **vpn-instance** *vpn-instance-name* ] ] | **zone** [ *zone-name* ] ] | *other-attack-type* } command to view the status and configuration of the attack defense functions.
- Run the **display firewall log configuration** command to view the global configuration of the log function.
- Run the **display firewall session** { **all** [ **verbose** ] | **number** }, **display firewall session protocol** { *protocol-number* | *protocol-name* } [ **source** *source-address* [ *source-port* ] ] [ **destination** *destination-address* [ *destination-port* ] ] [ **verbose** ], **display firewall session destination** *destination-address* [ *destination-port* ] [ **verbose** ], or **display firewall session source** *source-address* [ *source-port* ] [ **destination** *destination-address* [ *destination-port* ] ] [ **verbose** ] command to check the session table of the firewall.
- Run the **display firewall ipv6 session** { **all** [ **verbose** ] | **number** }, **display firewall ipv6 session protocol** { *protocol-number* | *protocol-name* } [ **source** *source-address* [ *source-port* ] ] [ **destination** *destination-address* [ *destination-port* ] ] [ **verbose** ], **display firewall ipv6 session destination** *destination-address* [ *destination-port* ] [ **verbose** ], or **display firewall ipv6 session source** *source-address* [ *source-port* ] [ **destination** *destination-address* [ *destination-port* ] ] [ **verbose** ] command to check the IPv6 session table of the firewall.
- Run the **display firewall app** { **servermap** | **session** } **table statistics** command to check statistics on firewall application entries.
- Run the **display firewall app session table** [ **application-protocol** { **dns** | **ftp** | **http** | **pptp** | **rtsp** | **sip** } ] [ **source-ip** *ip-address* [ *port-number* ] ] [ **destination-ip** *ip-address* [ *port-number* ] ] command to check the application session table.
- Run the **display session** { **all** [ **verbose** ] | **number** } or **display session destination** *destination-address* [ *destination-port* ] [ **verbose** ] or **display session source** *source-address* [ *source-port* ] [ **destination** *destination-address* [ *destination-port* ] ] [ **verbose** ] or **display session protocol** { *protocol-number* | *protocol-name* } [ **source** *source-address* [ *source-port* ] ]

 Copyright © Huawei Technologies Co., Ltd. 

[ **destination** *destination-address* [ *destination-port* ] ] [ **verbose** ] command to check the session table information.

**----End**

## 6.17.2 Clearing the Firewall Statistics

### Context

To view the communication packets of a device within a specified period, clear the previous packet statistics first.

### Procedure

- Run the **clear firewall statistics system normal** command in the system view to clear the statistics about normal packets in the system.
- Run the **clear firewall statistics zone** *zone-name* command in the system view to clear the statistics about normal packets in a zone.

**----End**

## 6.17.3 Clearing Statistics on Firewall Application Entries

### Context

You can clear existing statistics on firewall application entries when you need to collect new statistics. After you perform this task, all statistics on firewall application entries are cleared.

**NOTE**

Statistics on firewall application entries cannot be restored after they are cleared. Exercise caution when you use the command.

### Procedure

- Run the **reset firewall app** { **servermap** | **session** } **table statistics** command to clear statistics on firewall application entries.

**----End**

## 6.17.4 Clearing Attack Defense Statistics on Firewall

### Context

To collect attack defense statistics on the firewall, run this command to clear existing statistics first. After this command is run, attack defense statistics on the firewall are deleted.

**NOTE**

Attack defense statistics on the firewall cannot be restored after you clear them. So, confirm the action before you use the command.

 Copyright © Huawei Technologies Co., Ltd. 

### Procedure

- Run the **reset firewall statistics system defend** command to clear attack defense statistics on the firewall.

**----End**

# 6.18 Configuration Examples for Firewalls

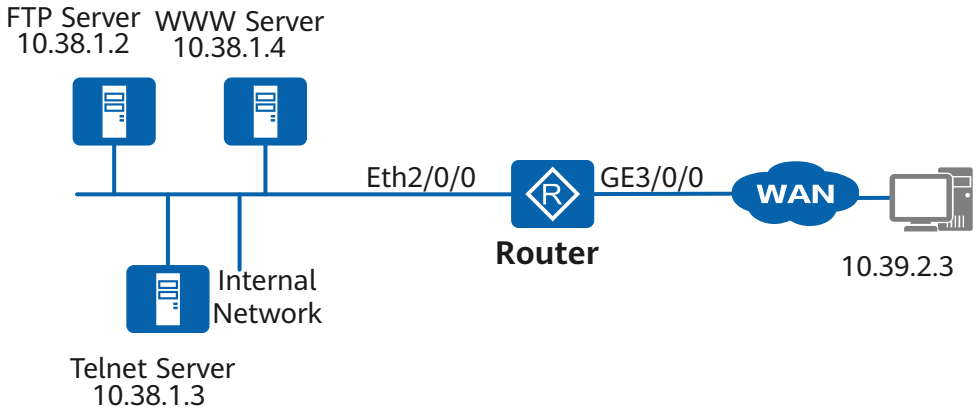
## 6.18.1 Example for Configuring the ACL-based Packet Filtering Firewall

### Networking Requirements

As shown in **Figure 6-22**, Eth2/0/0 of the Router is connected to a highly secure internal network, and GE3/0/0 is connected to an insecure external network. The Router must filter the packets between the internal network and the external network. The following requirements must be met:

- A host (10.39.2.3) on the external network is allowed to access the servers in the internal network.
- Other hosts are not allowed to access servers on the internal network.

**Figure 6-22** Network diagram for configuring ACL-based packet filtering




### Configuration Roadmap

The configuration roadmap is as follows:

1. Configure zones and an interzone.
2. Add interfaces to the zones.
3. Configure an ACL.
4. Configure ACL-based packet filtering in the interzone.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Configure zones and an interzone on the Router .

```
<Huawei> system-view
[Huawei] firewall zone trust
[Huawei-zone-trust] priority 14
[Huawei-zone-trust] quit
[Huawei] firewall zone untrust
[Huawei-zone-untrust] priority 1
[Huawei-zone-untrust] quit
[Huawei] firewall interzone trust untrust
[Huawei-interzone-trust-untrust] firewall enable
[Huawei-interzone-trust-untrust] quit
```

**Step 2** Add Router interfaces to zones.

```
[Huawei] vlan 100
[Huawei-vlan100] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 10.38.1.1 24
[Huawei-Vlanif100] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type access
[Huawei-Ethernet2/0/0] port default vlan 100
[Huawei-Ethernet2/0/0] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] zone trust
[Huawei-Vlanif100] quit
[Huawei] interface gigabitethernet 3/0/0
[Huawei-GigabitEthernet3/0/0] ip address 10.39.2.1 24
[Huawei-GigabitEthernet3/0/0] zone untrust
[Huawei-GigabitEthernet3/0/0] quit
```

**Step 3** Configure an ACL on the Router .

```
[Huawei] acl 3102
[Huawei-acl-adv-3102] rule permit tcp source 10.39.2.3 0.0.0.0 destination 10.38.1.2 0.0.0.0
[Huawei-acl-adv-3102] rule permit tcp source 10.39.2.3 0.0.0.0 destination 10.38.1.3 0.0.0.0
[Huawei-acl-adv-3102] rule permit tcp source 10.39.2.3 0.0.0.0 destination 10.38.1.4 0.0.0.0
[Huawei-acl-adv-3102] rule deny ip
[Huawei-acl-adv-3102] quit
```

**Step 4** Configure packet filtering on the Router .

```
[Huawei] firewall interzone trust untrust
[Huawei-interzone-trust-untrust] packet-filter 3102 inbound
[Huawei-interzone-trust-untrust] quit
```

**Step 5** Verify the configuration.

After the configuration is complete, only the specified host (10.39.2.3) can access servers on the internal network.

Run the **display firewall interzone** [ *zone-name1 zone-name2* ] command on the Router , and the result is as follows:

```
[Huawei] display firewall interzone trust untrust
interzone trust untrust
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
 packet-filter 3102 inbound
```

**----End**

## Configuration Files

Configuration file of the Router

 Copyright © Huawei Technologies Co., Ltd. 

```
#
 vlan batch 100
#
acl number 3102
 rule 5 permit tcp source 10.39.2.3 0 destination 10.38.1.2 0
 rule 10 permit tcp source 10.39.2.3 0 destination 10.38.1.3 0
 rule 15 permit tcp source 10.39.2.3 0 destination 10.38.1.4 0
 rule 20 deny ip
#
interface Vlanif100
 ip address 10.38.1.1 255.255.255.0
 zone trust
#
firewall zone trust
 priority 14
#
firewall zone untrust
 priority 1
#
firewall interzone trust untrust
 firewall enable
 packet-filter 3102 inbound
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 100
#
interface GigabitEthernet3/0/0
 ip address 10.39.2.1 255.255.255.0
 zone untrust
#
return
```

## 6.18.2 Example for Configuring ASPF and Port Mapping

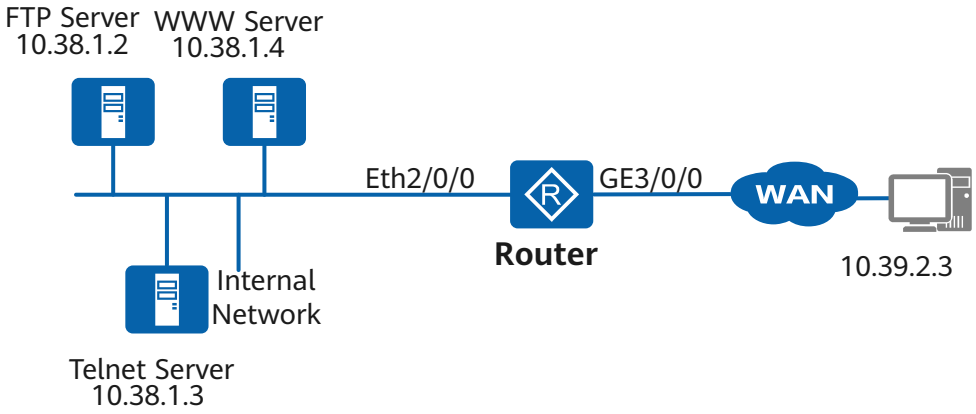
### Networking Requirements

As shown in **Figure 6-23**, Eth2/0/0 of the Router is connected to a highly secure internal network, and GE3/0/0 is connected to an insecure external network. The Router must filter the packets and perform ASPF check between the internal network and the external network. The following requirements must be met:

- A host (10.39.2.3) on the external network is allowed to access the servers in the internal network.
- Other hosts are not allowed to access servers on the internal network.
- The Router checks the FTP status of the connections and filters out undesired packets.
- The packets from the external host are sent to the FTP server through port 2121, which is used as the port of the FTP protocol.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 6-23** Network diagram of ASPF and port mapping




## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure zones and an interzone.
2. Add interfaces to the zones.
3. Configure ACLs.
4. Configure ACL-based packet filtering in the interzone.
5. Configure ASPF in the interzone.
6. Map port 2121 to the FTP protocol.

## Procedure

**Step 1** Configure zones and an interzone on the Router .

```
<Huawei> system-view
[Huawei] firewall zone trust
[Huawei-zone-trust] priority 14
[Huawei-zone-trust] quit
[Huawei] firewall zone untrust
[Huawei-zone-untrust] priority 1
[Huawei-zone-untrust] quit
[Huawei] firewall interzone trust untrust
[Huawei-interzone-trust-untrust] firewall enable
[Huawei-interzone-trust-untrust] quit
```

**Step 2** Add the interfaces of Router to zones.

```
[Huawei] vlan 100
[Huawei-vlan100] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 10.38.1.1 24
[Huawei-Vlanif100] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type access
[Huawei-Ethernet2/0/0] port default vlan 100
[Huawei-Ethernet2/0/0] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] zone trust
[Huawei-Vlanif100] quit
[Huawei] interface gigabitethernet 3/0/0
[Huawei-GigabitEthernet3/0/0] ip address 10.39.2.1 24
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Huawei-GigabitEthernet3/0/0] zone untrust
[Huawei-GigabitEthernet3/0/0] quit
```

**Step 3** Configure ACLs on Router .

```
[Huawei] acl 2102
[Huawei-acl-basic-2102] rule permit source 10.38.1.2 0.0.0.0
[Huawei-acl-basic-2102] quit
[Huawei] acl 3102
[Huawei-acl-adv-3102] rule permit tcp source 10.39.2.3 0.0.0.0 destination 10.38.1.2 0.0.0.0
[Huawei-acl-adv-3102] rule permit tcp source 10.39.2.3 0.0.0.0 destination 10.38.1.3 0.0.0.0
[Huawei-acl-adv-3102] rule permit tcp source 10.39.2.3 0.0.0.0 destination 10.38.1.4 0.0.0.0
[Huawei-acl-adv-3102] rule deny ip
[Huawei-acl-adv-3102] quit
```

**Step 4** Configure packet filtering on Router .

```
[Huawei] firewall interzone trust untrust
[Huawei-interzone-trust-untrust] packet-filter 3102 inbound
```

**Step 5** Configure ASPF on the Router .

```
[Huawei-interzone-trust-untrust] detect aspf ftp
[Huawei-interzone-trust-untrust] quit
```

**Step 6** Configure port mapping on the Router .

```
[Huawei] port-mapping ftp port 2121 acl 2102
```

**Step 7** Verify the configuration.

Run the **display firewall interzone** *zone-name1 zone-name2* command on the Router , and the command output is as follows:

```
[Huawei] display firewall interzone trust untrust
interzone trust untrust
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
 packet-filter 3102 inbound
 detect aspf ftp
```

Run the **display port-mapping ftp** command on the Router , and the command output is as follows:

```
[Huawei] display port-mapping ftp
  ------------------------------------------------
 Service    Port       Acl        Type
------------------------------------------------
 ftp          21                 system defined
 ftp        2121      2102         user   defined
------------------------------------------------
Total number is : 2
```

**----End**

## Configuration Files

Configuration file of the Router

```
#
vlan batch 100
#
acl number 2102
 rule 5 permit source 10.38.1.2 0
#
acl number 3102
 rule 5 permit tcp source 10.39.2.3 0 destination 10.38.1.2 0
 rule 10 permit tcp source 10.39.2.3 0 destination 10.38.1.3 0
 rule 15 permit tcp source 10.39.2.3 0 destination 10.38.1.4 0
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 rule 20 deny ip
#
port-mapping ftp port 2121 acl 2102
#
interface Vlanif100
 ip address 10.38.1.1 255.255.255.0
 zone trust
#
firewall zone trust
 priority 14
#
firewall zone untrust
 priority 1
#
firewall interzone trust untrust
 firewall enable
 packet-filter 3102 inbound
 detect aspf ftp
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 100
#
interface GigabitEthernet3/0/0
 ip address 10.39.2.1 255.255.255.0
 zone untrust
#
return
```

## 6.18.3 Example for Configuring the Blacklist

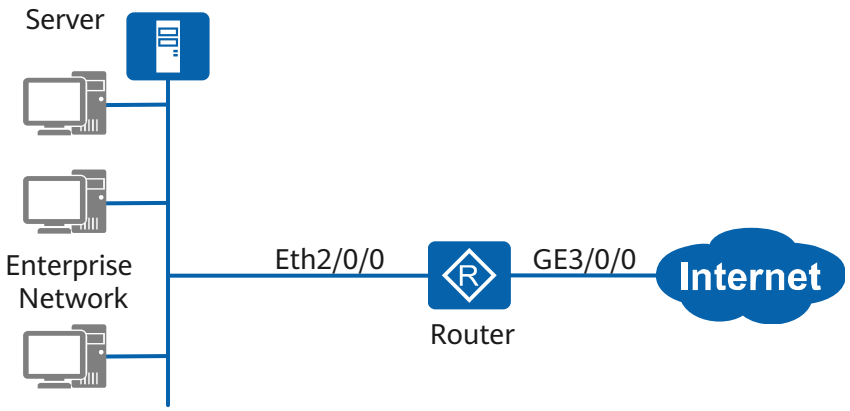
### Networking Requirements

As shown in **Figure 6-24**, Eth2/0/0 of the Router is connected to a highly secure internal network, and GE3/0/0 is connected to the insecure external network.

The Router needs to apply IP address sweeping defense and blacklist functions to the packets sent from the Internet to the enterprise intranet. If the Router detects that an IP address sweeping attack defense from an IP address, it adds the IP address to the blacklist. The maximum session rate is 5000 pps, and the blacklist timeout is 30 minutes.

If an IP address, for example, 1.1.1.2, attempts to attack the enterprise intranet multiple times, you can manually add the IP address to the blacklist. Then the IP address will be always in the blacklist.

**Figure 6-24** Network diagram of blacklist configuration




 Copyright © Huawei Technologies Co., Ltd. 

## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure zones and an interzone.
2. Add interfaces to the zones.
3. Enable the blacklist function.
4. Add an entry to the blacklist.
5. Enable the defense against IP address sweeping and port scanning.
6. Configure the maximum session rate and blacklist timeout for the defense against IP address sweeping and port scanning.

## Procedure

**Step 1** Configure zones and an interzone on the Router .

```
[Huawei] firewall zone trust
[Huawei-zone-trust] priority 14
[Huawei-zone-trust] quit
[Huawei] firewall zone untrust
[Huawei-zone-untrust] priority 1
[Huawei-zone-untrust] quit
[Huawei] firewall interzone trust untrust
[Huawei-interzone-trust-untrust] firewall enable
[Huawei-interzone-trust-untrust] quit
```

**Step 2** Add Router interfaces to zones.

```
[Huawei] vlan 100
[Huawei-vlan100] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 10.38.1.1 24
[Huawei-Vlanif100] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type access
[Huawei-Ethernet2/0/0] port default vlan 100
[Huawei-Ethernet2/0/0] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] zone trust
[Huawei-Vlanif100] quit
[Huawei] interface gigabitethernet 3/0/0
[Huawei-GigabitEthernet3/0/0] ip address 1.1.2.1 24
[Huawei-GigabitEthernet3/0/0] zone untrust
[Huawei-GigabitEthernet3/0/0] quit
```

**Step 3** Enable the blacklist function.

```
[Huawei] firewall blacklist enable
```

**Step 4** Add an entry to the blacklist.

```
[Huawei] firewall blacklist 1.1.1.2
```

**Step 5** Enable the defense against IP address sweeping and port scanning.

```
[Huawei] firewall defend ip-sweep enable
[Huawei] firewall defend port-scan enable
```

**Step 6** Configure the maximum session rate and blacklist timeout for the defense against IP address sweeping and port scanning.

```
[Huawei] firewall defend ip-sweep max-rate 5000
[Huawei] firewall defend ip-sweep blacklist-expire-time 30
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Huawei] firewall defend port-scan max-rate 5000
[Huawei] firewall defend port-scan blacklist-expire-time 30
```

**Step 7** Verify the configuration.

Run the **display firewall interzone** [ *zone-name1 zone-name2* ] command on the Router , and the command output is as follows:

```
[Huawei] display firewall interzone trust untrust
 interzone trust untrust
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
```

Run the **display firewall blacklist all** command on the Router , and the command output is as follows:

```
[Huawei] display firewall blacklist all
Firewall Blacklist Items :
------------------------------------------------------------------------------
IP-Address      Reason       Expire-Time(m) VPN-Instance
------------------------------------------------------------------------------
1.1.1.2      Manual       Permanent
------------------------------------------------------------------------------
 total number is : 1
```

Run the **display firewall defend** command on the Router , and the command output is as follows:

```
[Huawei] display firewall defend port-scan
  defend-flag              : enable
  max-rate                 : 5000  (pps)
  blacklist-expire-time    : 30    (m)

[Huawei] display firewall defend ip-sweep
  defend-flag              : enable
  max-rate                 : 5000  (pps)
  blacklist-expire-time    : 30    (m)
```

**----End**

## Configuration Files

Configuration file of the Router

```
#
 firewall defend ip-sweep enable
 firewall defend port-scan enable
 firewall defend ip-sweep max-rate 5000
 firewall defend ip-sweep blacklist-expire-time 30
 firewall defend port-scan max-rate 5000
 firewall defend port-scan blacklist-expire-time 30
#
 firewall blacklist enable
 firewall blacklist 1.1.1.2
#
vlan batch 100
#
interface Vlanif100
 ip address 10.38.1.1 255.255.255.0
 zone trust
#
firewall zone trust
 priority 14
#
firewall zone untrust
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 priority 1
#
firewall interzone trust untrust
 firewall enable
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 100
#
interface GigabitEthernet3/0/0
 ip address 1.1.2.1 255.255.255.0
 zone untrust
#
return
```

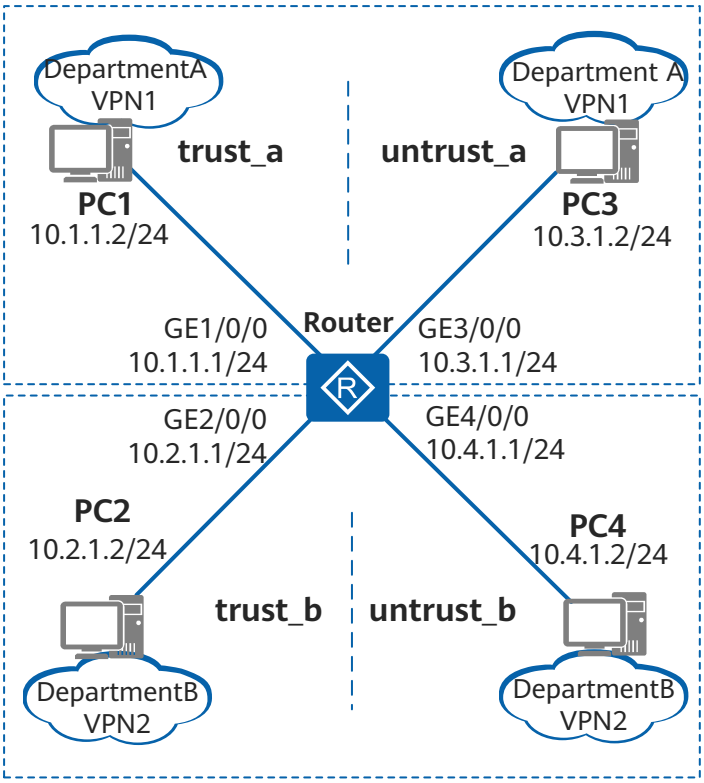
# 6.18.4 Example for Configuring Blacklists on Virtual Firewalls

## Networking Requirements

On the Router, virtual firewalls can be independently deployed on VPN instances.

As shown in **Figure 6-25**, virtual firewalls are configured for VPN instances on the Router to isolate department A and department B. Firewall policies are deployed independently and zones are configured for each VPN. Department A detects attack packets from 10.3.1.2 on VPN1. A blacklist needs to be configured on VPN1 to discard packets with source IP address 10.3.1.2.

**Figure 6-25** Networking diagram of blacklist configuration on virtual firewalls




 Copyright © Huawei Technologies Co., Ltd. 

## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure VPN instances on the Router to isolate department A from department B.
2. Configure zones on the Router.
3. Configure a blacklist for VPN1 on the Router to filter out packets with source IP address 10.3.1.2.

## Procedure

**Step 1** Configure VPN instances on the Router.

# Configure VPN instances **vpn1** and **vpn2** for department A and department B.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] ip vpn-instance vpn1
[Router-vpn-instance-vpn1] ipv4-family
[Router-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[Router-vpn-instance-vpn1-af-ipv4] quit
[Router-vpn-instance-vpn1] quit
[Router] ip vpn-instance vpn2
[Router-vpn-instance-vpn2] ipv4-family
[Router-vpn-instance-vpn2-af-ipv4] route-distinguisher 200:1
[Router-vpn-instance-vpn2-af-ipv4] quit
[Router-vpn-instance-vpn2] quit
```

# Bind VPN instances to private interfaces and configure private IP addresses as gateway addresses.

```
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip binding vpn-instance vpn1
[Router-GigabitEthernet1/0/0] ip address 10.1.1.1 255.255.255.0
[Router-GigabitEthernet1/0/0] quit
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] ip binding vpn-instance vpn2
[Router-GigabitEthernet2/0/0] ip address 10.2.1.1 255.255.255.0
[Router-GigabitEthernet2/0/0] quit
[Router] interface gigabitethernet 3/0/0
[Router-GigabitEthernet3/0/0] ip binding vpn-instance vpn1
[Router-GigabitEthernet3/0/0] ip address 10.3.1.1 255.255.255.0
[Router-GigabitEthernet3/0/0] quit
[Router] interface gigabitethernet 4/0/0
[Router-GigabitEthernet4/0/0] ip binding vpn-instance vpn2
[Router-GigabitEthernet4/0/0] ip address 10.4.1.1 255.255.255.0
[Router-GigabitEthernet4/0/0] quit
```

**Step 2** Configure zones on the Router.

# Configure zones and an interzone for **vpn1** on the Router.

```
[Router] firewall zone trust_a
[Router-zone-trust_a] priority 15
[Router-zone-trust_a] quit
[Router] firewall zone untrust_a
[Router-zone-untrust_a] priority 1
[Router-zone-untrust_a] quit
[Router] firewall interzone trust_a untrust_a
[Router-interzone-trust_a-untrust_a] firewall enable
[Router-interzone-trust_a-untrust_a] quit
```

# Configure zones and an interzone for **vpn2** on the Router.

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router] firewall zone trust_b
[Router-zone-trust_b] priority 30
[Router-zone-trust_b] quit
[Router] firewall zone untrust_b
[Router-zone-untrust_b] priority 5
[Router-zone-untrust_b] quit
[Router] firewall interzone trust_b untrust_b
[Router-interzone-trust_b-untrust_b] firewall enable
[Router-interzone-trust_b-untrust_b] quit
```

# On the Router, add interfaces to zones.

```
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] zone trust_a
[Router-GigabitEthernet1/0/0] quit
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] zone trust_b
[Router-GigabitEthernet2/0/0] quit
[Router] interface gigabitethernet 3/0/0
[Router-GigabitEthernet3/0/0] zone untrust_a
[Router-GigabitEthernet3/0/0] quit
[Router] interface gigabitethernet 4/0/0
[Router-GigabitEthernet4/0/0] zone untrust_b
[Router-GigabitEthernet4/0/0] quit
```

**Step 3** Configure the blacklist for **vpn1** on the Router.

# Enable the blacklist function.

```
[Router] firewall blacklist enable
```

# Add a blacklist entry in **vpn1**.

```
[Router] firewall blacklist 10.3.1.2 vpn-instance vpn1
```

**Step 4** Verify the configuration.

# After the configuration is complete, run the **display firewall interzone** command on the Router to view interzone policies.

```
[Router] display firewall interzone
 interzone trust_a untrust_a
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound

 interzone trust_b untrust_b
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound

 total number is : 2
```

# Run the **display firewall blacklist all** command on the Router to view blacklist information.

```
[Router] display firewall blacklist all
 Firewall blacklist items :
------------------------------------------------------------------------------
IP-Address      Reason       Expire-Time(m) VPN-Instance
------------------------------------------------------------------------------
10.3.1.2        Manual       Permanent      vpn1
------------------------------------------------------------------------------
 Total number is : 1
```

# Packets of PC3 cannot pass through virtual firewall **vpn1**.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## Configuration Files

Configuration file of the Router

```
#
 sysname Router
#
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 100:1
#
ip vpn-instance vpn2
 ipv4-family
  route-distinguisher 200:1
#
firewall zone trust_a
 priority 15
#
firewall zone trust_b
 priority 30
#
firewall zone untrust_a
 priority 1
#
firewall zone untrust_b
 priority 5
#
firewall interzone trust_a untrust_a
 firewall enable
#
firewall interzone trust_b untrust_b
 firewall enable
#
 firewall blacklist enable
 firewall blacklist 10.3.1.2 vpn-instance vpn1
#
interface GigabitEthernet1/0/0
 ip binding vpn-instance vpn1
 ip address 10.1.1.1 255.255.255.0
 zone trust_a
#
interface GigabitEthernet2/0/0
 ip binding vpn-instance vpn2
 ip address 10.2.1.1 255.255.255.0
 zone trust_b
#
interface GigabitEthernet3/0/0
 ip binding vpn-instance vpn1
 ip address 10.3.1.1 255.255.255.0
 zone untrust_a
#
interface GigabitEthernet4/0/0
 ip binding vpn-instance vpn2
 ip address 10.4.1.1 255.255.255.0
 zone untrust_b
#
return
```

# 6.18.5 Example for Configuring Firewall HSB

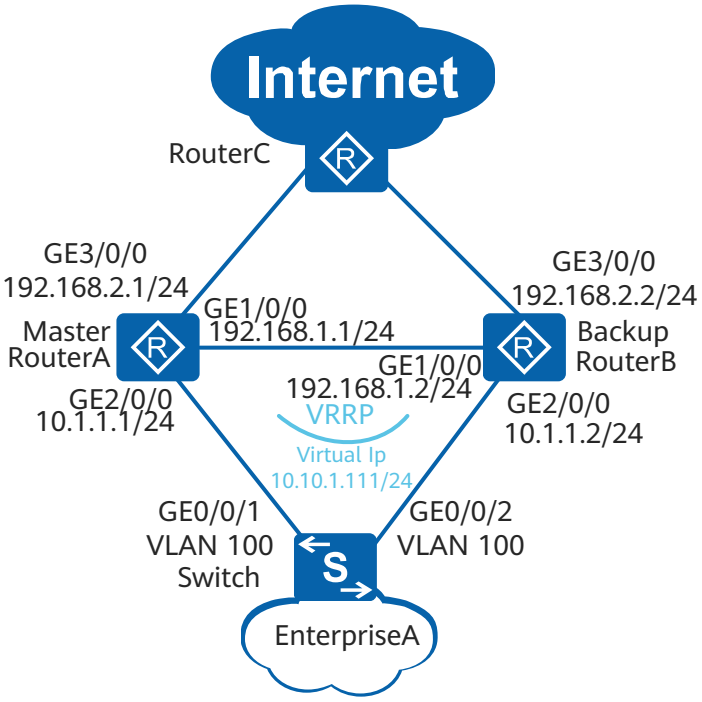
## Networking Requirements

To ensure enterprise intranet security, Enterprise A deploys a firewall between the intranet and extranet. All traffic must pass through the firewall device; therefore, the firewall device failure leads to interruption of all traffic. To enhance network reliability, Enterprise A deploys two firewall devices in HSB mode to ensure

 Copyright © Huawei Technologies Co., Ltd. 

uninterrupted network upon the failure of a firewall device, as shown in **Figure 6-26**.

**Figure 6-26** Networking diagram for configuring firewall HSB




## Configuration Roadmap

In normal cases, hosts in Enterprise A use RouterA as the default gateway to access the Internet. When RouterA becomes faulty, RouterB takes over services on RouterA. The configuration roadmap is as follows:

1. Assign an IP address to each interface of devices and configure a routing protocol on each device to ensure network connectivity.
2. Configure the firewall function on RouterA and RouterB to implement security isolation between the enterprise intranet and extranet.
3. Configure VRRP groups on RouterA and RouterB. Configure a high priority for RouterA as the master device to forward traffic, and a low priority for RouterB as the backup device.
4. Configure the HSB function for RouterA and RouterB so that service information on RouterA is backed up to RouterB in batches in real time, ensuring smooth service switchover from the master device to the backup device.
5. Enable the firewall HSB function on RouterA and RouterB so that the backup firewall device RouterB starts the firewall function upon RouterA failure, ensuring non-stop network running.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Configure devices to ensure network connectivity.

# Assign an IP address to each interface on RouterA. The configuration on RouterB is similar to that on RouterA.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.1.1.1 24
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.2.1 24
[RouterA-GigabitEthernet3/0/0] quit
```

# Configure Layer 2 transparent transmission on Switch.

```
<Huawei> system-view
[Huawei] sysname Switch
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[Switch-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port hybrid pvid vlan 100
[Switch-GigabitEthernet0/0/2] port hybrid untagged vlan 100
[Switch-GigabitEthernet0/0/2] quit
```

**Step 2** Configure the firewall function.

# Configure the firewall function for RouterA. The configuration on RouterB is similar to that on RouterA.

```
[RouterA] firewall zone trust
[RouterA-zone-trust] priority 15
[RouterA-zone-trust] quit
[RouterA] firewall zone untrust
[RouterA-zone-untrust] priority 1
[RouterA-zone-untrust] quit
[RouterA] firewall interzone trust untrust
[RouterA-interzone-trust-untrust] firewall enable
[RouterA-interzone-trust-untrust] quit
```

# Add an interface on RouterA to the security zone. The configuration on RouterB is similar to that on RouterA.

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] zone untrust
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] zone trust
[RouterA-GigabitEthernet2/0/0] quit
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] zone untrust
[RouterA-GigabitEthernet3/0/0] quit
```

**Step 3** Configure VRRP groups.

# Create VRRP group 1 on RouterA and set the VRRP priority to 120.

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.111
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[RouterA-GigabitEthernet2/0/0] vrrp vrid 1 priority 120
[RouterA-GigabitEthernet2/0/0] quit
```

# Create VRRP group 1 on RouterB and set the VRRP priority to 100.

```
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.111
[RouterB-GigabitEthernet2/0/0] quit
```

**Step 4** Configure the HSB function and enable HSB for the firewall devices.

# Create HSB service 0 on RouterA and configure the IP addresses and port numbers for the local and peer devices.

```
[RouterA] hsb-service 0
[RouterA-hsb-service-0] service-ip-port local-ip 192.168.1.1 peer-ip 192.168.1.2 local-data-port 10241
peer-data-port 10241
[RouterA-hsb-service-0] quit
```

# Create HSB service 0 on RouterB and configure the IP addresses and port numbers for the local and peer devices.

```
[RouterB] hsb-service 0
[RouterB-hsb-service-0] service-ip-port local-ip 192.168.1.2 peer-ip 192.168.1.1 local-data-port 10241
peer-data-port 10241
[RouterB-hsb-service-0] quit
```

# Create HSB group 0 on RouterA, and bind HSB group 0 to VRRP group 1. The configuration on RouterB is similar to that on RouterA.

```
[RouterA] hsb-group 0
[RouterA-hsb-group-0] bind-service 0
[RouterA-hsb-group-0] track vrrp vrid 1 interface gigabitethernet 2/0/0
[RouterA-hsb-group-0] quit
```

# Enable the firewall function for RouterA. The configuration on RouterB is similar to that on RouterA.

```
[RouterA] hsb-service-type firewall hsb-group 0
```

# Enable HSB group 0 on RouterA to make it take effect. The configuration on RouterB is similar to that on RouterA.

```
[RouterA] hsb-group 0
[RouterA-hsb-group-0] hsb enable
[RouterA-hsb-group-0] quit
```

**Step 5** Verify the configuration.

# Run the **display hsb-group** *group-index* command on RouterA and RouterB to check the HSB group running status. The command output on Router A and Router B is as follows:

```
<RouterA> display hsb-group 0
Hot Standby Group Configuration:
-------------------------------------------------------------
  HSB-group ID               : 0
  Vrrp Group ID              : 1
  Vrrp Interface             : GigabitEthernet2/0/0
  Service Index              : 0
  Group Vrrp Status          : Master
  Group Status               : Active
  Group Backup Process       : Realtime
  Peer Group Device Name     : Router
  Peer Group Software Version : V200R010
  Group Backup Modules       : Firewall
```

 Copyright © Huawei Technologies Co., Ltd. 

```
<RouterB> display hsb-group 0
Hot Standby Group Configuration:
-------------------------------------------------------------
  HSB-group ID               : 0
  Vrrp Group ID              : 1
  Vrrp Interface             : GigabitEthernet2/0/0
  Service Index              : 0
  Group Vrrp Status          : Backup
  Group Status               : Inactive
  Group Backup Process       : Realtime
  Peer Group Device Name     : Router
  Peer Group Software Version : V200R010
  Group Backup Modules       : Firewall
```

# Run the **shutdown** command on an interface GE2/0/0 of RouterA to simulate a fault on RouterA.

```
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] shutdown
[RouterA-GigabitEthernet2/0/0] quit
```

# Run the **display hsb-group** *group-index* command on RouterB to check the HSB group status. The command output shows that RouterB is Master.

```
<RouterB> display hsb-group 0
Hot Standby Group Configuration:
-------------------------------------------------------------
  Hsb-group ID               : 0
  Vrrp Group ID              : 1
  Vrrp Interface             : GigabitEthernet2/0/0
  Service Index              : 0
  Group Vrrp Status          : Master
  Group Status               : Independent
  Group Backup Process       : Realtime
  Peer Group Device Name     : Router
  Peer Group Software Version : V200R010
  Group Backup Modules       : Firewall
```

**----End**

## Configuration Files

- RouterA configuration file

```
#
sysname RouterA
#
hsb-service-type firewall hsb-group 0
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
 zone untrust
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 120
 zone trust
#
interface GigabitEthernet3/0/0
 ip address 192.168.2.1 255.255.255.0
 zone untrust
#
hsb-service 0
 service-ip-port local-ip 192.168.1.1 peer-ip 192.168.1.2 local-data-port 10241 peer-data-port 10241
#
firewall zone trust
 priority 15
#
```

 Copyright © Huawei Technologies Co., Ltd. 

```
firewall zone untrust
 priority 1
#
firewall interzone trust untrust
 firewall enable
#
hsb-group 0
 track vrrp vrid 1 interface GigabitEthernet2/0/0
 bind-service 0
 hsb enable
#
return
```

- RouterB configuration file

```
#
sysname RouterB
#
hsb-service-type firewall hsb-group 0
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
 zone untrust
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 zone trust
#
interface GigabitEthernet3/0/0
 ip address 192.168.2.2 255.255.255.0
 zone untrust
#
firewall zone trust
 priority 15
#
firewall zone untrust
 priority 1
#
firewall interzone trust untrust
 firewall enable
#
hsb-service 0
 service-ip-port local-ip 192.168.1.2 peer-ip 192.168.1.1 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
 track vrrp vrid 1 interface GigabitEthernet2/0/0
 bind-service 0
 hsb enable
#
return
```

- Configuration file of Switch

```
#
sysname Switch
#
vlan batch 100
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

 Copyright © Huawei Technologies Co., Ltd. 

# 6.19 FAQ About Firewalls

## 6.19.1 How Do I Delete and View the Firewall and NAT Flow Table?

Run the **reset session all** command in the system view to clear the firewall and NAT flow table.

Run the **display session** command in any view to check the firewall and NAT flow table.

## 6.19.2 How Can I View the ACL Hit Count Configured on the Packet Filtering Firewall?

1. In the system view, run the **traffic classifier** *classifier-name* command to create a traffic classifier and access the traffic classifier view. Run the **if-match acl** *{ acl-number | acl-name }* command to configure ACL rules for traffic classification.
2. In the system view, run the **traffic behavior** *behavior-name* command to create a traffic behavior and access the traffic behavior view. Run the **statistic enable** command to enable the traffic statistics function.
3. In the system view, run the **traffic policy** *policy-name* command to create a traffic policy and access the traffic policy view. Run the **classifier** *classifier-name* **behavior** *behavior-name* command to associate a traffic classifier and a traffic behavior with the traffic policy.
4. In the interface view, run the **traffic-policy** *policy-name* **inbound** command.
5. Run the **display traffic policy statistics interface** *interface-type interface-number* **inbound verbose rule-base** command to view the ACL hit count configured on the packet filtering firewall.

## 6.19.3 Which Protocols Does the AR Firewall ASPF Support?

The following protocols are supported:

- File Transfer Protocol (FTP)
- Session Initiation Protocol (SIP)
- Real-Time Streaming Protocol (RTSP)

## 6.19.4 What Are the Types of Blacklists? (Firewall)

There are two types of blacklists:

- Static blacklists that are configured manually.
- Dynamic blacklists that are generated when the system detects scanning attacks.

 Copyright © Huawei Technologies Co., Ltd. 

# 7 Deep Security Defense Configuration

## About This Chapter

The device uses security policies to provide deep security defense based on the application layer. It protects users against attacks from various network threats.

7.1 Security Policy
The device uses security policies to forward service traffic and implement integrated content security detection and processing.

7.2 IPS Configuration
An intrusion prevention system (IPS) is a security mechanism. IPS detects intrusion behaviors by monitoring or analyzing system events, and terminates the intrusion behaviors in real time through certain response methods.

7.3 URL Filtering Configuration
Uniform Resource Locator (URL) filtering regulates online behaviors by controlling which URLs users can access.

## 7.1 Security Policy

The device uses security policies to forward service traffic and implement integrated content security detection and processing.

### 7.1.1 Overview of Security Policies

With the network development, increasing new applications bring more conveniences to people's network life, but also cause more security risks. When internal hosts access the Internet, worms, Trojan horses, and other viruses may be introduced accidentally from the Internet and cause confidential data leakage and huge losses to enterprises. To protect the internal network security, enterprises must identify and monitor traffic contents on the basis of controlling traffic sources and destinations. However, traditional single packet detection mechanism only analyzes the security of a single packet, and cannot defend against network threats such as buffer overflow attacks, Trojan horses, and worms that occur during a normal network access process. A security policy not only forwards

 Copyright © Huawei Technologies Co., Ltd. 

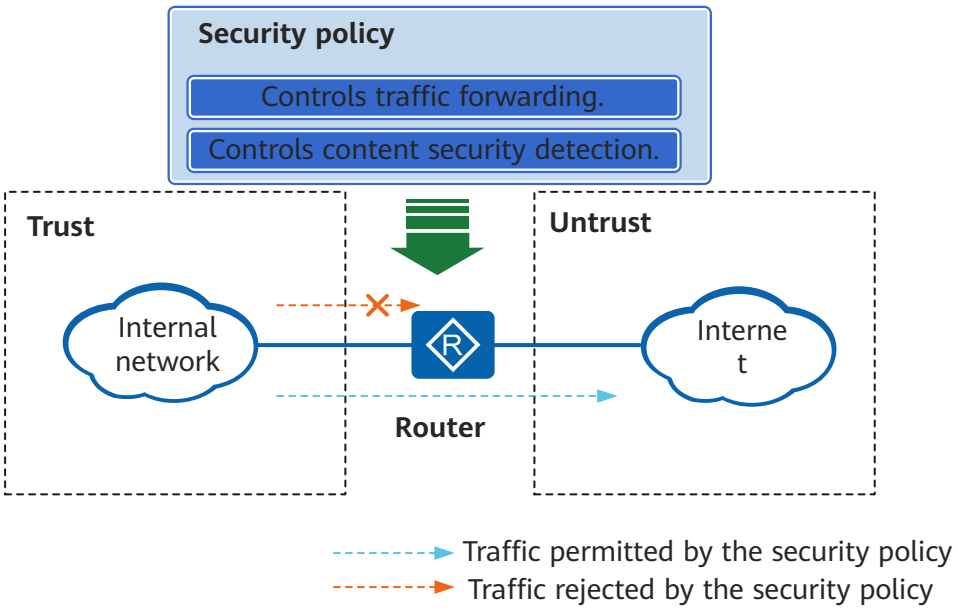
network traffic, but also implements integrated content security detection on network traffic.

In integrated content security detection, the device uses the intelligent awareness engine to detect and process traffic contents only once, and implements content security functions including the IPS, URL filtering. The integrated detection is highly efficient. You can configure broad security policy conditions to match a type of traffic, and ensure the network security using various content security functions.

As shown in **Figure 7-1**, the device can identify traffic attributes and match the attributes with security policy conditions. If all conditions are matched, the traffic matches the security policy successfully. Otherwise, the traffic is allowed to pass through. After traffic matches the security policy, the device implements content security detection on the traffic, and performs corresponding actions according to the detection result.

- If the detection result is permit or alarm, the traffic is allowed to pass through. If the detection result is alarm, the device records a log.
- If the detection result is blocking, the traffic is not allowed to pass through.

**Figure 7-1** Security policy of the router




## 7.1.2 Understanding Security Policies

### Security Policies of the Device

Traditional firewalls control traffic using IP addresses and protocols. With the network development, increasing new applications bring more conveniences to people's network life, but also cause more security risks. Typically, with the web technology development, more and more services with different risk levels run on ports 80 and 443 using HTTP and HTTPs, including web instant communication, web games, video websites, and web chat. In addition, new working methods such as telecommuting and mobile office emerge. IP addresses of hosts used by the

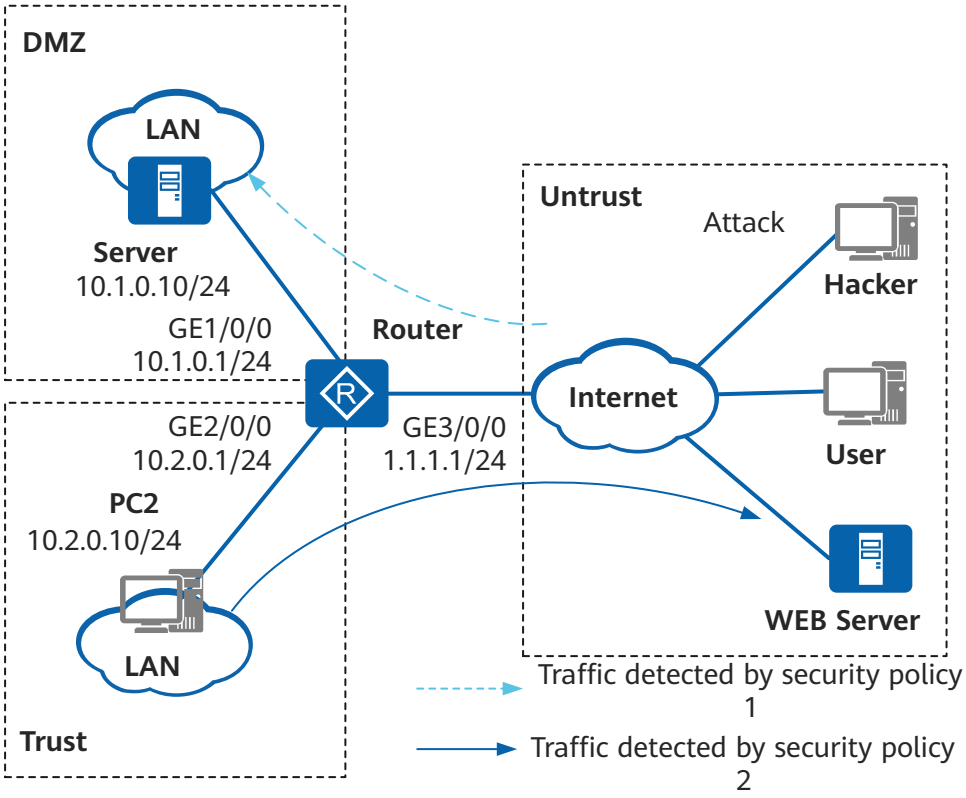

Copyright © Huawei Technologies Co., Ltd.

same user may change at any time. Traffic control based on IP addresses cannot meet modern network requirements. Therefore, traffic contents must be identified and monitored in enterprises' network security management on the basis of controlling traffic sources and destinations.

The device uses security policies to forward and control traffic at the application layer, and implements content security detection and processing on traffic. Security policies of the device adapt to modern network characteristics and meet modern network requirements.

As shown in **Figure 7-2**, the device uses security policy 1 to apply the intrusion prevention system (IPS) function to protect the internal server against attacks from the Internet. The device uses security policy 2 to apply the IPS function and URL filtering function to allow users in the Trust zone to browse the Internet. The device also detects contents browsed by users and defends against viruses and hackers.

**Figure 7-2** Security policies of the device




After using security policies, the device has the following advantages:

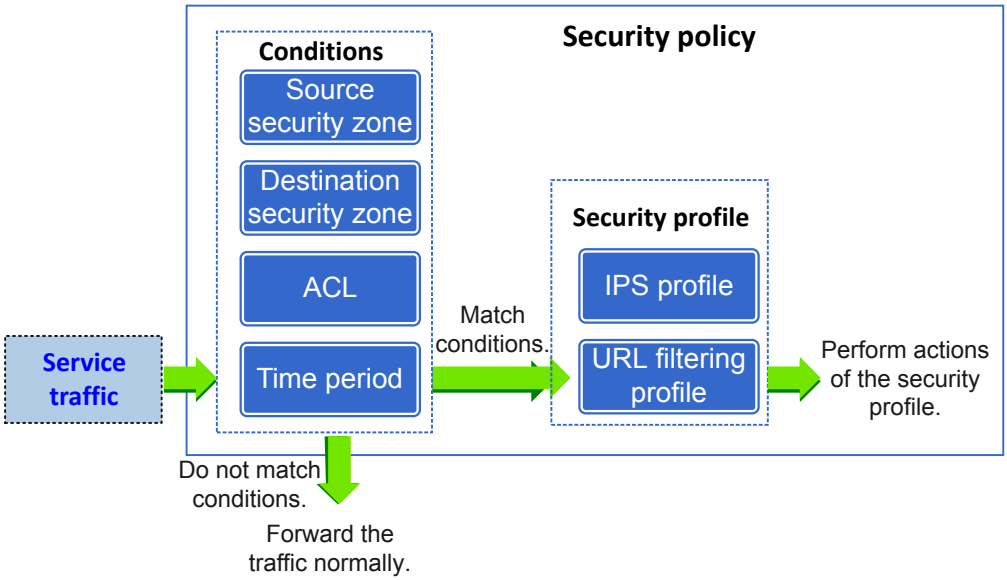
- The device applies corresponding security policies in different security zones, making the network management more flexible and visualized.
- The device effectively differentiates different applications (such as web instant communication and web games) carried by a protocol (such as HTTP), providing more refined network management.
- The device uses security policies to implement content security detection, blocking viruses and hackers to protect the internal network.

 Copyright © Huawei Technologies Co., Ltd. 

## Security Policy Processing Flow

Figure 7-3 shows the processing flow of security policies on the device.

**Figure 7-3** Security policy processing flow




When traffic passes through the Router, the security policy processing flow is as follows:

1. The Router detects received traffic and obtains traffic attributes including the source security zone, destination security zone, ACL (source IP address, destination IP address, source port, destination port, and protocol type), and time period.
2. The Router matches traffic attributes with security policy conditions. If all conditions are matched, go to step 3. Otherwise, the traffic is allowed to pass through.
3. If the traffic matches security policy conditions successfully, the Router determines whether security policies reference security profiles. If security profiles are referenced, go to step 4. If no security profile is referenced, the traffic is allowed to pass through.
4. If security policies reference security profiles, the Router implements integrated content security detection on the traffic.

   In the integrated detection, the device only detects traffic contents once according to security profile conditions, and implements security profile actions according to the detection result. If one security profile blocks the traffic, the Router blocks the traffic. If all security profiles allow the traffic to pass through, the Router forwards the traffic.

   As shown in Figure 7-4, all content security functions of the Router are implemented through security profiles referenced by security policies.


Copyright © Huawei Technologies Co., Ltd.

Detection and processing are only performed once, greatly improving the system performance.

**Figure 7-4** Integrated detection of the Router

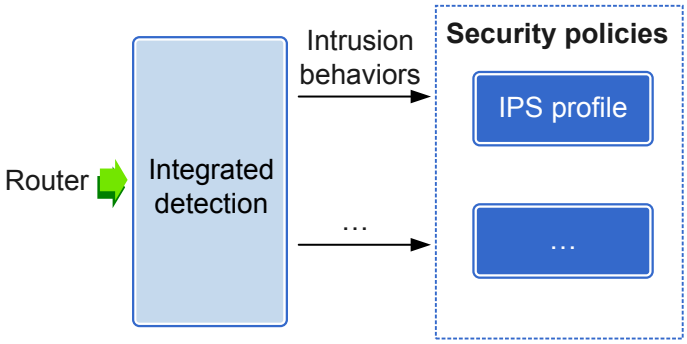



Table 7-1 describes security profiles that can be referenced by security policies and their functions.

**Table 7-1** Security profiles and functions

| Security Profile | Function |
| --- | --- |
| 7.2 IPS Configuration | An intrusion prevention system (IPS) implements attack detection by comparing traffic contents with the IPS signature database. IPS effectively defends against attacks from the application layer, such as buffer overflow attacks, Trojan horses, and worms. |
| 7.3 URL Filtering Configuration | Manages and controls user's URL requests. It permits or rejects access to some web resources to control online behaviors. |

## Using Different Security Profiles Together

You can use different security profiles together to provide strong content security protection functions and avoid wasting system resources.

Table 7-2 describes some tips for using different security profiles together.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 7-2** Tips for using different security policies together

| Function | Purpose | Security Profile |
| --- | --- | --- |
| Server protection | Protects servers providing access to external networks against viruses and intrusion behaviors. | • IPS: defends against attacks from the application layer to servers. |
| Web access protection | Protects internal users against viruses and intrusion behaviors when they visit websites and download files. | • IPS: blocks intrusion behaviors in web access.<br>• URL filtering: filters illegal websites and malicious websites, and reduces risks of virus infection and attacks. |

## 7.1.3 Application Scenarios for Security Policies

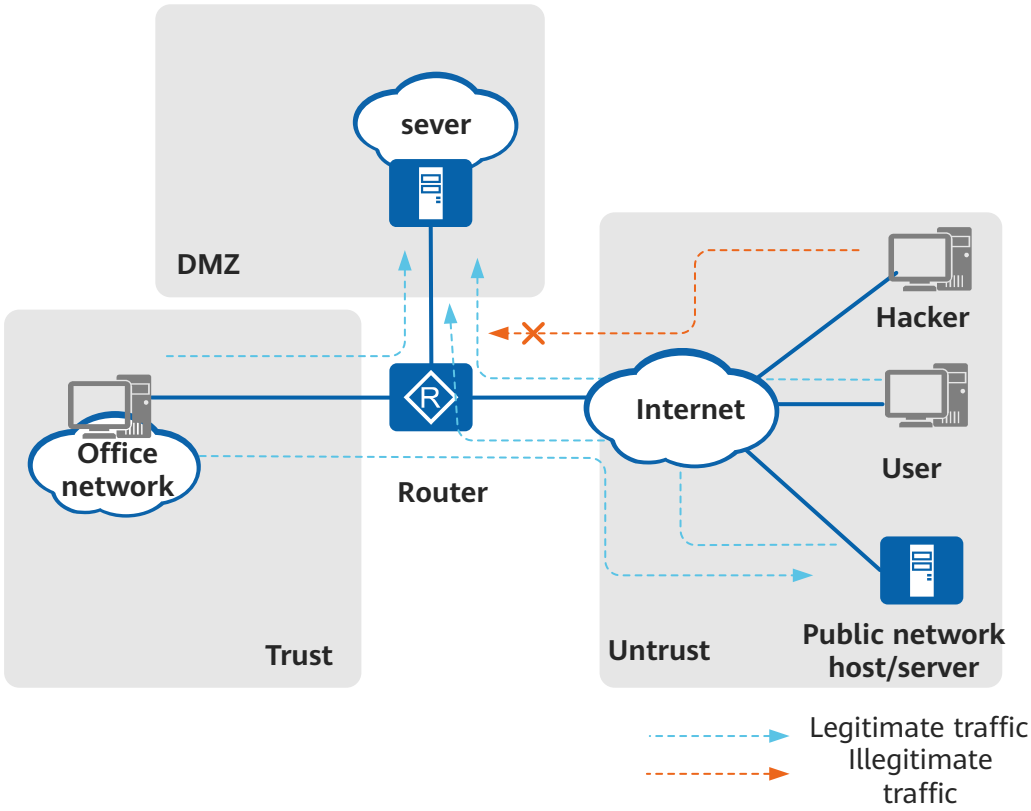
Multiple types of service traffic exist on the network. You can configure multiple security policies on the device for different service traffic. The device uses security policies to detect traffic between security zones, protecting enterprises' internal networks.

As shown in **Figure 7-5**, when the Router functions as the security gateway on the border of a large- and medium-sized enterprise's network, the security policy deployment is as follows:

- The enterprise deploys the office network, server network, and external network in different security zones. Configure security policies to detect traffic between security zones and protect the internal network.
- Configure content security functions of security policies according to the type of network services provided by the enterprise to the external network. For example, enable IPS on all servers.
- Configure the URL filtering security function when internal employees access the external network. The function prevents employees from visiting non-work-related websites during working hours and affecting the work efficiency.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 7-5** Applying security policies between the internal network and external network




# 7.2 IPS Configuration

An intrusion prevention system (IPS) is a security mechanism. IPS detects intrusion behaviors by monitoring or analyzing system events, and terminates the intrusion behaviors in real time through certain response methods.

## 7.2.1 Overview of IPS

### Definition

An intrusion prevention system (IPS) is a security mechanism. IPS detects intrusion behaviors (such as buffer overflow attacks, Trojan horses, and worms) by analyzing network traffic, and terminates the intrusion behaviors in real time through certain response methods. This protects enterprise information systems and network architectures against intrusions.

### Purpose

With the network development, increasing new applications bring more conveniences to people's network life, but also cause more security risks. When users access the Internet, worms, Trojan horses, and other viruses may be introduced accidentally from the Internet and cause confidential data leakage and

 Copyright © Huawei Technologies Co., Ltd. 

huge losses to enterprises. Therefore, traffic contents must be identified and monitored in enterprises' network security management on the basis of controlling traffic sources and destinations.

IPS can prevent attacks or intrusions at the application layer such as buffer overflow attacks, Trojan horses, and worms.

## Highlights

Intrusion prevention on the NGFW detects and automatically discards the intrusion packets or blocks the attack sources. Intrusion prevention on the NGFW has the following benefits:

- Real-time attack blocking: Deployed in in-line mode, the NGFW blocks the attack traffic in real time.
- In-depth protection: The NGFW examines the application-layer contents of packets, reassembles packets to analyze the protocols and detect threats, and blocks the attack packets based on the attack type and policy.
- All-round protection: Intrusion prevention defends against such attacks as worms, viruses, Trojan horses, botnets, spyware, adware, Common Gateway Interface (CGI), cross-site scripting, injection, directory traversal, information leaks, remote file inclusion, overflow, code execution, denial of service, scanning, and backdoors.
- Internal and external prevention: Intrusion prevention on the NGFW protects the intranet against both internal and external attacks. The system detects traffic that passes through, protecting both servers and clients.
- Constant update for up-to-date protection: The intrusion prevention signature database is constantly updated to identify the latest threats. You can periodically update the signature database from the update center.

## Difference from the IDS

Intrusion Detection System (IDS) detects abnormal traffic and suspicious traffic, generates alarms to notify the administrator of the network condition, and provides solutions accordingly. The IDS is a security function for risk management. Compared with the IDS, intrusion prevention not only detects attacks and malicious behavior to networks and data but also quickly terminates them. It is a security function for risk control.

Intrusion prevention provides advanced defense functions based on the traditional IDS.

- The IDS cannot defend against application-layer attacks, whereas the intrusion prevention device can.

  The IDS has high false negative and false positive ratios and generates a considerable number of logs and alarms, making it difficult to locate real attacks. The intrusion prevention device can remove outer layers of packets, identify protocols, resolve packets, classify the resolved packets, and match the packets with signatures to ensure the detection accuracy.
- The IDS device can detect attacks, but cannot prevent them. To prevent attacks, the IDS device must interwork with a firewall.

 Copyright © Huawei Technologies Co., Ltd. 

However, the intrusion prevention device can detect and block attacks. When detecting any attack, the intrusion prevention device automatically discards the attack packets or blocks the attack source.

## 7.2.2 Understanding IPS

### Concepts

Before understanding IPS, you need to understand functions of the IPS signature database, IPS signature, and Security Center Platform.

- IPS signature database: An IPS signature database invented by Huawei after analyzing various common intrusion behaviors. The IPS signature database defines the characteristics of various common intrusion behaviors, and assigns a unique intrusion behavior ID to each kind of intrusion behavior. After being loaded with the IPS signature database, the device can identify intrusion behaviors defined in the database.
- Security Center Platform: The domain name is **sec.huawei.com**. A server provided by Huawei to offer upgrade services of the IPS signature database for customers who purchase a license. For information about IPS signature database upgrade, see **IPS Signature Database Upgrade**.
- IPS signature:

  The IPS signature is used to describe the characteristics of the intrusion behavior on the network. The device can detect and defend against attacks from the intrusion behavior by comparing packet contents with IPS signatures.

  IPS signatures include predefined signatures and user-defined signatures.

  – Predefined signatures

    Predefined signatures are a large number of signatures that are predefined by the system. A predefined signature presets the default action of the signature as blocking or alarm. Administrators can prevent or block intrusion behaviors based on the predefined signatures.

    The device is loaded with the IPS signature database before delivery. To identify the latest intrusion behaviors in real time, you can purchase and activate a license. The IPS signature database updates on time. You can continuously obtain the latest IPS signature database from the Security Center Platform to ensure timely response to new intrusion behaviors.

  – User-defined signatures

    User-defined signatures are created by the administrator according to the characteristics of intrusion behaviors. The administrator creates such signatures in the following scenarios:

    ▪ When the administrator wants to reject or record a certain behavior that is not included in predefined signatures. For example, when the administrator wants to forbid staff to transmit executable files (which are prone to virus) but the executable file forbidden behavior is not defined in the predefined signatures, the administrator can create a signature according to the behavior characteristics, set the action to block, and import the created signature to the configuration file.

    ▪ When the network is undergoing an attack but the IPS signature database has not been updated, the administrator can create a

 Copyright © Huawei Technologies Co., Ltd. 

signature for the attack according to the attack characteristics. After the IPS signature database is updated, the created signature takes effect.

You can use the signature filter to manage user-defined signatures, and use the exception signatures to manage user-defined signatures and IPS signatures.

- Signature filter

  A large number of signatures flood the signature database after updates. By analyzing the features of common threats, you can summarize signatures that contain these features and add these signatures to a signature filter.

  A collection of signatures that meet specified filtering conditions. Filtering conditions of the signature filter include the signature category, target, protocol, severity, and operating system. Only signatures that meet all filtering conditions can be added to the signature filter. For example, if only HTTP packets need to be defended against, you can only configure the HTTP protocol as the filtering condition. Then the signature that meets the filtering condition is added to the signature filter.

  The action of a signature filter can be **Block**, **Alert**, or **Default** (use the default actions of signatures). The action of a signature filter has a higher priority than the default actions of signatures in the filter.

  Signature filters configured earlier have higher priorities. If two signature filters in one security profile contain the same signature, packets matching the signature are processed according to the signature filter configured earlier.

- Exception signature

  To facilitate management, the signature filter filters signatures in batches. If administrators need to configure actions for some signatures different from actions of the signature filter, they can add the signatures to exception signatures and configure actions for the signatures independently. For example, when detecting an attack through logs, the administrator can add the signature that matches the attack to exception signatures and configure a block action for the signature.

  The action of a signature exception can be **Block**, **Alert**, **Allow**.

  The action of a signature exception has a higher priority than that of a signature filter. If a signature matches a signature exception and a signature filter, the action of the signature exception takes effect.

  For example, the actions for a batch of signatures in the signature filter are **block**. Then the device blocks an R&D software requested by an employee. The log indicates that the R&D software matches a signature in the signature filter and is blocked because of false positive. In such cases, add the signature as an exception and set the action to **Allow**.

## IPS Signature Database Upgrade

The IPS signature database supports incremental online upgrade. Services are not affected during the online upgrade. After the IPS signature database is upgraded, the system automatically switches the IPS signature database version, and the device does not need to be restarted. If an error occurs during the IPS signature database upgrade and causes an upgrade failure, the system automatically rolls back to the previous IPS signature database version, and normal services are not affected.

 Copyright © Huawei Technologies Co., Ltd. 

To ensure timely response to new intrusion behaviors, the IPS signature database on the Security Center Platform updates in real time. You can use the Security Center Platform upgrade method or local upgrade method to obtain the latest IPS signature database upgrade package from the Security Center Platform, achieving the best protection effect against intrusions.

- Online upgrade:
  - If the device can access the Security Center Platform, you can upgrade through the Security Center Platform.
  - If the device cannot access the Security Center Platform, and the internal upgrade server can access, you can upgrade through the internal server.

    You can use the internal upgrade server to connect to the Security Center Platform to obtain the IPS signature database, and use the internal upgrade server to upload the upgrade file to the device for the IPS signature database upgrade.

  You can upgrade online periodically or immediately.
  - Scheduled upgrade: You only need to specify a fixed time for scheduled upgrade. The IPS signature database can update automatically and timely. To avoid upgrade failure caused by bad network conditions, you are advised to set the upgrade time to a time when network traffic is low.
  - Immediate upgrade: When administrators detect new attacks on the network and the configured upgrade time is not reached, the upgrade is performed immediately so that the device can defend against new attacks.
- Local upgrade: When the device cannot be connected to the Security Center Platform through the network, you can log in to the Security Center Platform to download the latest IPS signature database upgrade package, save the package to a local PC, and then upload the upgrade file to the device through FTP, TFTP, or web to upgrade the IPS signature database.

## Traffic Processing Flow

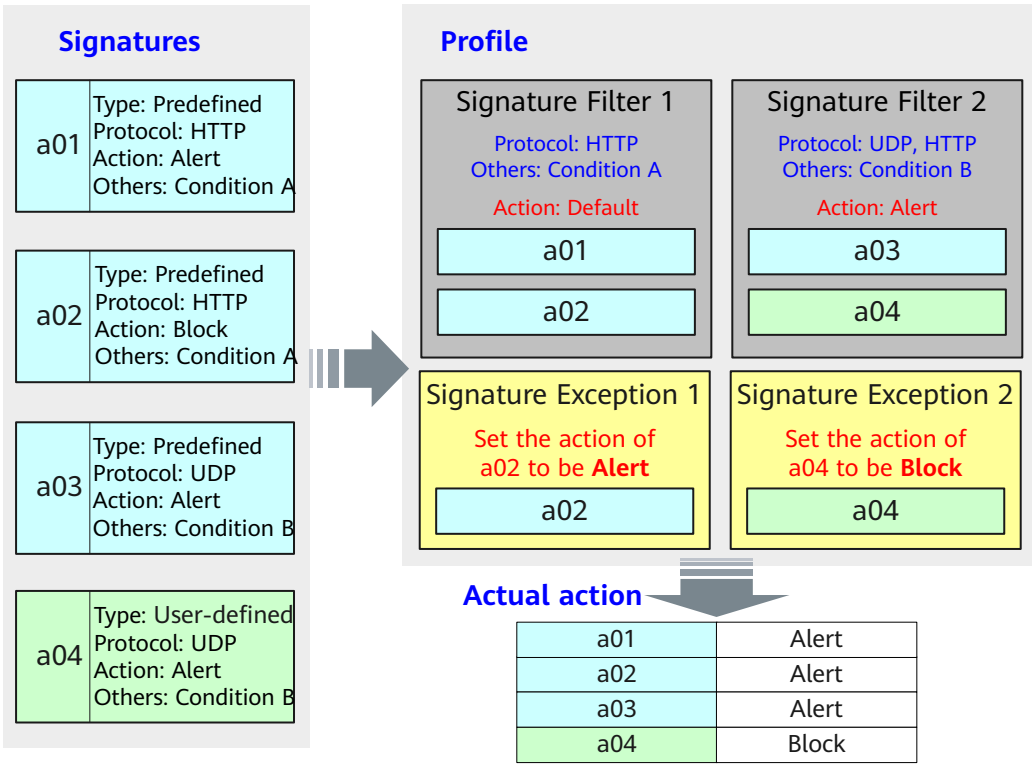
An intrusion prevention profile contains multiple signature filters and exception signatures.

**Figure 7-6** shows the relationship between signatures, signature filters, and exception signatures. In this example, a01, a02, and a03 are predefined signatures. a04 is a user-defined signature. Two signature filters are configured in the profile. Signature filter 1 filters signatures a01 and a02 whose protocol set is set to HTTP and other filtering conditions are set to condition A. The action for signature filter 1 is set to the default action for signatures. Signature filter 2 filters a03 and a04 whose protocol set is set to HTTP or UDP and other filtering conditions are set to condition B. The action for signature filter 2 is set to alert. Besides, two exception signatures are configured in the profile. In exception signature 1, set the action for a02 to alert. In exception signature 2, set the action for a04 to block.

The actual action for a signature is jointly determined by the default action for the signature, action for the signature filter, and action for the exception signature. For details, see **Actual action** in **Figure 7-6**.

 Copyright © Huawei Technologies Co., Ltd. 

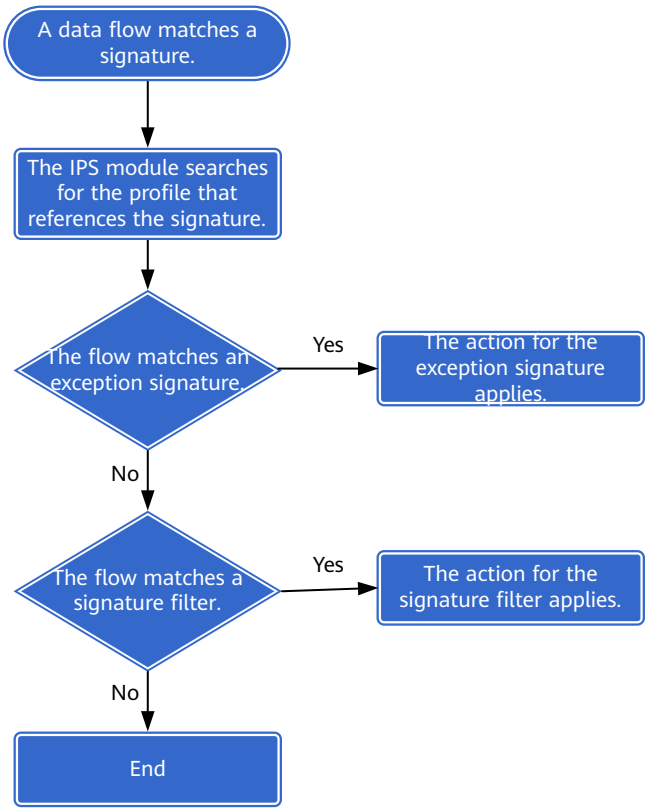
**Figure 7-6** Relationship between signatures, signature filters, and exception signatures




When a data flow matches the intrusion prevention profile, the device sends the data flow to the intrusion prevention module to match the signatures referenced by the profile one by one. **Figure 7-7** shows the traffic processing flow.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 7-7** Traffic processing flow




NOTE

When a packet matches multiple signatures, the actual action for the packet is as follows:

- If the actions for all the matched signatures are **Alert**, the action for the packet is **Alert**.
- If the action for any matched signature is **Block**, the action for the packet is **Block**.

When a data flow matches multiple signature filters, the action for the signature filter with the highest priority is performed on the data flow.

Using signatures in **Figure 7-6** as an example, assume that a packet matches signature a02 in exception signature 1. According to the processing flow, the action for exception signature 1 is **Alert**, not **Block**. Then the packet continues to match the signature filter. Assume that the packet matches signature a04 in signature filter 2. The action for signature filter 2 is **Block**. Then the actual action for the packet is **Block**. That is, the device discards the packet.

## 7.2.3 Application Scenarios for IPS

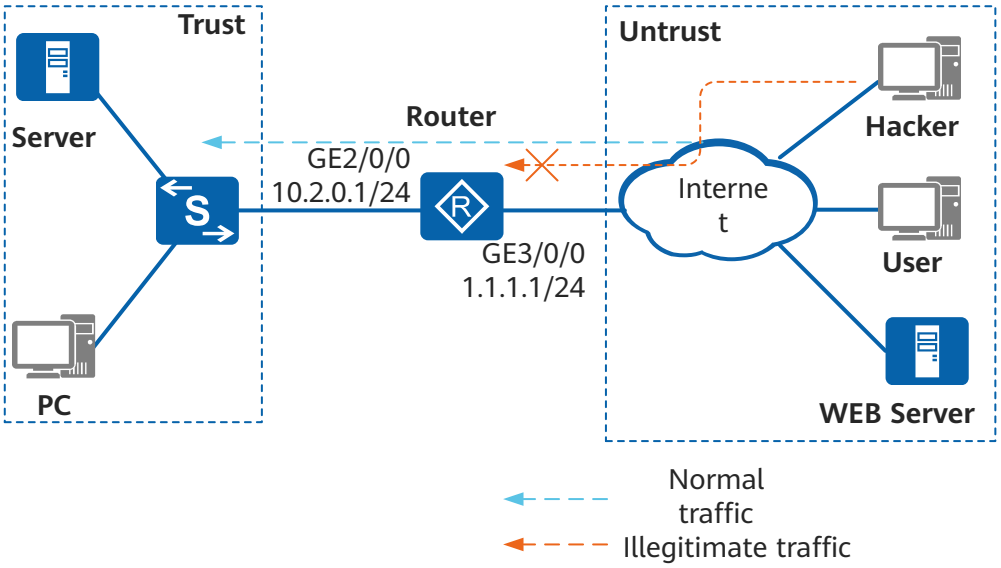
### 7.2.3.1 Using IPS to Block Intrusion Behaviors

As shown in **Figure 7-8**, the router is the enterprise egress gateway. IPS can be deployed on the router to defend against attacks (such as buffer overflow attacks, Trojan horses, and worms) at the application layer, protect internal hosts against viruses and intrusions from the external network, and improve the enterprise network security. The router then detects traffic between the security zones. When

 Copyright © Huawei Technologies Co., Ltd. 

detecting intrusion behaviors in the traffic, the router blocks the illegitimate traffic. If no intrusion behavior is detected, the traffic is allowed to pass through.

**Figure 7-8** Typical IPS usage scenario




## 7.2.4 Licensing Requirements and Limitations for IPS

### Involved Network Elements

Other network elements are not required.

### Licensing Requirements

For IPS-capable devices, their licensing requirements for the IPS function are as follows:

- AR160&AR1200&AR2200&AR3200 series: By default, this function is disabled on a new device. To use the IPS function, apply for and purchase the following license from the Huawei local office.
  - AR160 series: AR150&160&200 Value-Added Security Package
  - AR1200 series: AR1200 Value-Added Security Package
  - AR2200 series: AR2200 Value-Added Security Package
  - AR3200 series: AR3200 Value-Added Security Package

For IPS signature database upgrade-capable devices, their licensing requirements for the IPS signature database upgrade function are as follows:

- AR160&AR1200&AR2200&AR3200 series: By default, this function is disabled on a new device. To use the IPS signature database upgrade function, apply for and purchase the following license from the Huawei local office.
  - AR160 series: AR160 IPS Service Subscribe 1 Year
  - AR1200 series: AR1200 IPS Service Subscribe 1 Year

 Copyright © Huawei Technologies Co., Ltd. 

  - AR2200 series: AR2200 IPS Service Subscribe 1 Year
  - AR3200 series: AR3200 IPS Service Subscribe 1 Year

### Feature Limitations

When deploying IPS on the router, pay attention to the following:

- The device supports IPS filtering that involves personal communication information collection or storage. Huawei will not collect or save user communication information independently. You must use the features in compliance with applicable laws and regulations. Ensure that your customers' privacy is protected when you are collecting or saving communication information.
- In a networking environment in which the inbound and outbound paths of packets are different, IPS probably cannot detect network intrusions effectively.
- The following product models support IPS function:
  - AR160 series: AR169BF, AR169FGW-L, AR169FGVW-L, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169EGW-L, AR169EW, AR168F-4P, AR161EW, AR161EW-M1, AR161FW, AR161FV-1P, and AR169FVW.
  - AR1200 series: AR1220E, AR1220EV, and AR1220EVW.
  - AR2200 series: AR2204, AR2204XE, AR2204XE-DC, AR2220, AR2220E, AR2240, and AR2240C.
  - AR3200 series: All models.

## 7.2.5 Default Settings for IPS

Table 7-3 describes the default settings for IPS.

**Table 7-3** Default settings for IPS

| Parameter | Default Setting |
| --- | --- |
| Security policy | Unspecified |

 Copyright © Huawei Technologies Co., Ltd. 

| Parameter | Default Setting |
| --- | --- |
| IPS profile | The device has multiple default intrusion prevention profiles for different application scenarios. The default intrusion prevention profiles can be displayed, cloned, or referenced in security policies, but cannot be modified or deleted.<br>• **strict**: It contains all signatures and the action is block. Apply to all protocols and categories. The intrusion prevention profile applies to the scenarios in which the device is required to block all matched packets.<br>• **web_server**: It contains all signatures and the action is the default actions. Apply to DNS, HTTP, FTP protocols and all categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a web server.<br>• **file_server**: It contains all signatures and the action is the default actions. Apply to DNS, SMB, NETBIOS, NFS, SUNRPC, MSRPC, FILE, TELNET protocols and all categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a file server.<br>• **dns_server**: It contains all signatures and the action is the default actions. Apply to DNS protocol and all categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a DNS server.<br>• **mail_server**: It contains all signatures and the action is the default actions. Apply to DNS, IMAP4, SMTP, POP3 protocols and all categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a mail server.<br>• **inside_firewall**: It contains all signatures and the action is the |

 Copyright © Huawei Technologies Co., Ltd. 

| Parameter | Default Setting |
| --- | --- |
| | default actions. Apply to all protocols and categories. The intrusion prevention profile applies to the scenarios in which the device is deployed behind a firewall.<br>• **dmz**: It contains all signatures and the action is the default actions. Apply to all protocols except NETBIOS, NFS, SMB, TELNET TFTP and categories. The intrusion prevention profile applies to the scenarios in which the device is deployed behind a firewall. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a DMZ.<br>• **outside_firewall**: It contains all signatures and the action is the default actions. Apply to all protocols and categories except Scanner. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a firewall.<br>• **ids**: It contains all signatures and the action is alert. Apply to all protocols and categories. The intrusion prevention profile applies to the scenarios in which the device is deployed offline as an IDS.<br>• **default**: It contains all signatures and the action is the default actions. Apply to all protocols and categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in-line as an IPS. |
| IPS log caching function | Enabled. |
| Output time of IPS logs in the cache | 1 minute. |

# 7.2.6 Enabling the Deep Security Function

## Context

To use the IPS or URL filtering function, you need to purchase a license and run the **engine enable** command to enable the deep security function.


Copyright © Huawei Technologies Co., Ltd.

To disable deep security, run the **undo engine enable** command, and restart the device. After the device restarts, the deep security configurations are deleted.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **engine enable**

The deep security function is enabled.

By default, the system disables the deep security function.

NOTE

If the **engine enable** command is executed for the first time, you need to run the **update restore sdb-default** command to manually load the signature file.

**----End**

## 7.2.7 Updating the IPS Signature Database

### Prerequisites

Ensure that the license has been activated and is within the effective service period.

After purchasing the license with the intrusion prevention upgrade function, you can obtain the signature database that contains predefined signatures, and continuously gain new intrusion prevention versions from the Security Center Platform (the default domain name is sec.huawei.com) to update the signature database.

### Context

To improve security protection capability of the system, update the IPS signature database before configuring the IPS function. The device can identify more intrusion behaviors with the latest IPS signature database.

The IPS signature database is the basis for IPS to perform intrusion defense detection. The IPS signature database contains predefined IPS signatures. IPS signatures are used to describe features of intrusion behaviors on the network. The device compares packet contents with IPS signatures for detection and attack defense. If a data flow matches the features in a signature, the device processes the data flow according to the signature action. The contents of predefined signatures are fixed and cannot be created or modified.

You can update the database in the following methods:

- Online upgrade

  If the device can access the Security Center Platform, you can upgrade through the Security Center Platform.
- Local upgrade

  When the device cannot be connected to the Security Center Platform through the network, you can log in to the Security Center Platform to

 Copyright © Huawei Technologies Co., Ltd. 

download the latest IPS signature database upgrade package, save the package to a local PC, and then upload the upgrade file to the device through FTP, TFTP, or web to upgrade the IPS signature database.

NOTE

- Because the signature database is not installed on the device, you must obtain the IPS license, and then download it to your local computer or install it online.
- When the startup path is changed, you must load the signature library again through online or local upgrade.

## Procedure

- Online upgrade
  a. Run **system-view**

     The system view is displayed.
  b. (Optional) Run **update server** { **domain** *domain-name* | **ip** *ip-address* } [ **port** *port-number* ]

     The IP address or domain name of the update server is configured.

     By default, the domain name of the update server is sec.huawei.com, and the port number is 80.
  c. Visit the upgrade server through the proxy server.
     i. Run **update proxy enable**

        The signature database proxy update function is enabled.

        By default, the signature database proxy update function is disabled.
     ii. Run **update proxy** { **domain** *domain-name* | **ip** *ip-address* } [ **port** *port-number* ] [ **user** *user-name* [ **password** *password* ] ]

        The IP address or domain name of the proxy server is configured.
  d. Update the IPS signature database using the Security Center Platform or the internal upgrade server.
     - Upgrade through the Security Center Platform.

       To allow the device to access the Security Center Platform, configure the DNS function on the device.

       1) Run **dns resolve**

          The DNS function is enabled.

       2) Run **dns server** *ip-address*

          An IP address is configured for the DNS server.
  e. Scheduled upgrade
     i. Run **update schedule ips-sdb enable**

        The scheduled upgrade function of the IPS signature database is enabled.

        By default, the scheduled online upgrade function of the IPS signature database is enabled.
     ii. Run **update schedule** [ { **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time* ]

 Copyright © Huawei Technologies Co., Ltd. 

The fixed online upgrade time of the IPS signature database is set.

If no fixed upgrade time is set, a time between 22:00 and 08:00 is selected randomly as the daily upgrade time by default.

It is recommended that you set *time* to the time when the device has the minimum traffic volume, for example, 6:00 am.

iii. Set the installation mode of the IPS signature database.

An IPS signature database can take effect only after it is installed on a device. You can select the installation mode, that is, whether confirmation is needed. If you select the confirmation mode, the device asks you whether to install the IPS signature database before the upgrade is performed.

The switching of new and old IPS signature databases will affect the intrusion detection effect. You can confirm the installation when the service traffic volume is small.

- Installation after confirmation

  1) Run **update confirm ips-sdb enable**

  The installation confirmation function is enabled. The upgrade file downloaded at a fixed time will be installed after confirmation.

  By default, the manual confirmation of database installation is disabled. That is, the device automatically installs the upgrade files after downloading them.

  2) Run **update apply ips-sdb**

  The downloaded upgrade file is installed.

- Installation without the need of confirmation

  Run **undo update confirm ips-sdb enable**

  The installation confirmation function is disabled. The upgrade file downloaded at a fixed time will be installed automatically without confirmation.

f. (Optional) Immediate upgrade

Generally, scheduled upgrade can meet service requirements. However, if new intrusion behaviors occur on the network but the update time is not reached, you can select immediate upgrade.

i. Run **update online ips-sdb**

The IPS signature database is upgraded immediately.

ii. Run **update apply ips-sdb**

The downloaded upgrade file is installed.

- Terminate upgrade

If the update occupies too many network resources, you can run the command to terminate the update.

NOTE

The update can be terminated only during file downloading.

a. Run **system-view**

 Copyright © Huawei Technologies Co., Ltd. 

The system view is displayed.

b. Run **update abort**

The upgrade is terminated.

- Version rollback

  If an error occurs after the update or the new IPS signature database does not meet your requirements, use this command to roll back the database.

  NOTE

  Before the version rollback, you are advised to run the **display version ips-sdb** command to view the information about the rollback version. Then, you can choose whether to perform the version rollback. If no rollback version is available, the version rollback fails. The version in the device remains unchanged.

  a. Run **system-view**

  The system view is displayed.

  b. Run **update rollback ips-sdb**

  The IPS signature database version is rolled back to the last version.

- Local upgrade

  a. Run **system-view**

  The system view is displayed.

  b. Run **update local ips-sdb file** *filename*

  The IPS signature database is upgraded locally.

  NOTE

  **Terminate upgrade** are not supported in the offline upgrade.

- Version Restore

  NOTE

  If the signature database is restored to the factory default version, all other versions on the device are deleted.

  a. Run **system-view**

  The system view is displayed.

  b. Run **update restore sdb-default ips-sdb**

  The IPS signature database is restored to the factory default version.

**----End**

## Verify the update result

- Run the **display engine information** command to view the status of engines and the version of all signature databases.
- Run the **display version ips-sdb** command to view version information of the IPS signature database.
- Run the **display update status** command to view the update status.
- Run the **display update configuration** command to view the update configuration.

 Copyright © Huawei Technologies Co., Ltd. 

# 7.2.8 Configuring IPS

## 7.2.8.1 (Optional) Configuring User-Defined Signatures

### Context

User-defined signatures are created by the administrator according to the characteristics of intrusion behaviors. The administrator creates such signatures in the following scenarios:

- When the administrator wants to reject or record a certain behavior that is not included in predefined signatures. For example, when the administrator wants to forbid staff to transmit executable files (which are prone to virus) but the executable file forbidden behavior is not defined in the predefined signatures, the administrator can create a signature according to the behavior characteristics, set the action to block, and import the created signature to the configuration file.
- When the network is undergoing an attack but the IPS signature database has not been updated, the administrator can create a signature for the attack according to the attack characteristics. After the IPS signature database is updated, the created signature takes effect.

A user-defined IPS signature consists of multiple rules, and each rule contains multiple conditions.

The device matches packets against the rules in the configuration sequence. When a packet matches one rule in a signature, the packet matches the signature. When a packet matches all conditions in a rule, the packet matches the rule.

NOTE

A user-defined IPS signature takes effect for all security policies on the device. After a security policy is applied to a security interzone, the user-defined signature takes effect immediately.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **ips signature-id** *signature-id*

A user-defined IPS signature is created and the IPS signature view is displayed.

By default, no user-defined IPS signature exists on the device.

**Step 3** (Optional) Run **name** *name*

The name of the user-defined signature is set.

**Step 4** (Optional) Run **description** *description*

The description of the user-defined signature is configured.

By default, no description is configured for a user-defined signature.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 5** Configure the basic characteristics of the user-defined signature.

- Run **target** { **both** | **client** | **server** }

  The detection target of the user-defined signature is specified.

  By default, the user-defined signatures are used to detect the packets on clients and servers.
- Run **severity** { **high** | **information** | **low** | **medium** }

  The severity of the user-defined signature is set.

  By default, the severity of a user-defined signature is high.
- Run **protocol** *protocol-name*

  The protocol type of the user-defined signature is set.

  By default, the protocol type of a user-defined signature is HTTP.

  NOTE

  A user-defined signature can have only one protocol type.
- Run **action** { **alert** | **block** }

  The action of the user-defined signature is set.

  By default, the action of a user-defined signature is alert.

**Step 6** Configure rules for a user-defined signature.

1. Run **rule name** *name*

   A user-defined signature rule is created and the rule view is displayed.

   By default, no user-defined signature rule exists on the device.

   NOTE

   To facilitate memorization and management, rename the user-defined signature rule.

   To rename the user-defined signature rule and enter the view of the rule, run the **rename** *new-name* command.
2. Run **scope** { **flow** | **message** | **packet** }

   The matching scope of user-defined signature rules is specified.

   By default, the matching scope of user-defined signature rules is **packet**.
3. Run **condition** [ *condition-id* ] **field** *field-name* **operate** { **equal** | **gthan** | **lthan** | **noequal** } **value** *value-content*

   The conditions of user-defined signature rules are specified.

   By default, no condition is configured for user-defined signature rules.

   At most four conditions can be configured for a rule.
4. Specify the matching order of user-defined signature rules.

   a. Run **check** { **random-order** | **sequential** }

   The matching order of user-defined signature rules is specified.

   By default, the matching order is **random-order**.

   NOTE

   After the **sequential** parameter is specified, only the packets matching the conditions in the ascending order of condition IDs are considered as intrusion packets. However, some intrusion packets do not match the conditions in sequence. These intrusion packets will be ignored.

 Copyright © Huawei Technologies Co., Ltd. 

b. (Optional) When the matching order is set to **sequential**, run:

The condition locations are adjusted.

5. (Optional) Run **source-ip** { [ **ipv4** ] *ip-address* | **any** }

The source IP address of user-defined signature rules is specified.

By default, any source IP address is checked by the user-defined signature rule.

6. (Optional) Run **source-port** { *start-port end-port* | **any** }

The source port of user-defined signature rules is specified.

By default, all source ports are checked.

7. (Optional) Run **destination-ip** { [ **ipv4** ] *ip-address* | **any** }

The destination IP address of user-defined signature rules is specified.

By default, any destination IP address is checked by the user-defined signature rule.

8. (Optional) Run **destination-port** { *start-port end-port* | **any** }

The destination port of user-defined signature rules is specified.

By default, all destination ports are checked.

**Step 7** (Optional) Run **quit**

Exit from the User-defined IPS signature rule view.

**Step 8** (Optional) Run **quit**

Exit from the IPS signature view.

**Step 9** (Optional) Run **ips signature-state** [ **signature-id** *signature-id* ] { **enabled** | **disabled** }

The state of user-defined signature is configured.

By default, the state of user-defined signature is not specified.

**Step 10** Run **condition move** *condition-id* **to** *new-condition-id*
**engine configuration commit**

Deliver the configuration.

**----End**

## 7.2.8.2 Configuring IPS Profiles

## Context

After the IPS signature database is loaded, a large number of signatures dynamically generated by files in the IPS signature database are not categorized, and features contained in some signatures do not exist on the local network. You need to use the signature filter to filter signatures in batches and configure unified actions. To configure specified actions for some signatures, administrators need to add the signatures to exception signatures.

You can configure IPS profiles to solve the preceding problem. One IPS profile can be configured with multiple signature filters and multiple exception signatures.

 Copyright © Huawei Technologies Co., Ltd. 

After being configured with signature filters and exception signatures, IPS profiles can filter signatures that are suitable for the local network. The device can use IPS profiles to defend against intrusion behaviors.

The device has multiple default intrusion prevention profiles for different application scenarios. The default intrusion prevention profiles can be displayed, cloned, or referenced in security policies, but cannot be modified or deleted.

- **strict**: It contains all signatures and the action is block. Apply to all protocols and categories. The intrusion prevention profile applies to the scenarios in which the device is required to block all matched packets.
- **web_server**: It contains all signatures and the action is the default actions. Apply to DNS, HTTP, FTP protocols and all categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a web server.
- **file_server**: It contains all signatures and the action is the default actions. Apply to DNS, SMB, NETBIOS, NFS, SUNRPC, MSRPC, FILE, TELNET protocols and all categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a file server.
- **dns_server**: It contains all signatures and the action is the default actions. Apply to DNS protocol and all categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a DNS server.
- **mail_server**: It contains all signatures and the action is the default actions. Apply to DNS, IMAP4, SMTP, POP3 protocols and all categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a mail server.
- **inside_firewall**: It contains all signatures and the action is the default actions. Apply to all protocols and categories. The intrusion prevention profile applies to the scenarios in which the device is deployed behind a firewall.
- **dmz**: It contains all signatures and the action is the default actions. Apply to all protocols except NETBIOS, NFS, SMB, TELNET TFTP and categories. The intrusion prevention profile applies to the scenarios in which the device is deployed behind a firewall. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a DMZ.
- **outside_firewall**: It contains all signatures and the action is the default actions. Apply to all protocols and categories except Scanner. The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a firewall.
- **ids**: It contains all signatures and the action is alert. Apply to all protocols and categories. The intrusion prevention profile applies to the scenarios in which the device is deployed offline as an IDS.
- **default**: It contains all signatures and the action is the default actions. Apply to all protocols and categories. The intrusion prevention profile applies to the scenarios in which the device is deployed in-line as an IPS.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 2** Create an IPS profile and enter the IPS profile view.

- Create an IPS profile without any configuration.

  Run **profile type ips name** *name*

  An IPS profile is created and the IPS profile view is displayed.

- Create an IPS profile by copying another profile.

  Run **profile type ips copy** *old-name* [ *new-name* ]

  An IPS profile is created by copying an existing IPS profile and the IPS profile view is displayed.

  The *old-name* has been created.

By default, the device has the IPS profile. The name is strict, web_server, file_server, dns_server, mail_server, inside_firewall, dmz, outside_firewall, ids and default.

NOTE

To facilitate IPS profile management, you can rename the IPS profile.

Run the command **rename** *new-name* to rename an existing IPS profile and displays the new IPS profile view.

**Step 3** (Optional) Run **collect-attack-evidence enable**

The attack evidence collection function of IPS is enabled.

By default, the attack evidence collection function of IPS is disabled.

NOTE

The log sending function of the IPS module has been enabled using the **engine log ips enable** command.

**Step 4** (Optional) Run **description** *description*

The description of an IPS profile is configured to identify the IPS profile.

By default, no description is configured for an IPS profile.

**Step 5** (Optional) Run **cnc domain-filter enable** [ **action** { **alert** | **block** } ]

The domain name-based filtering function is enabled.

By default, domain name-based filtering is disabled.

After domain name-based filtering is enabled, the default action is alert for packets matching the specified condition.

The domain name-based filtering function enables the device to filter out packets using the malicious domain name signature database.

NOTE

- Because the CNC is not installed on the device, you must obtain the IPS license, and then download the CNC to your local computer from sec.huawei.com or install the CNC online.
- When the startup path is changed, you must load the signature library again from sec.huawei.com through online or local upgrade.

**Step 6** Run **signature-set name** *name*

 Copyright © Huawei Technologies Co., Ltd. 

An IPS signature filter is created in the IPS profile view and the IPS signature filter view is displayed.

By default, no IPS signature filter is configured.

An IPS profile can be configured with multiple IPS signature filters.

NOTE

To facilitate IPS signature filter management, you can rename the user-defined IPS signature filters.

Run the command **rename** *new-name* to rename an existing IPS signature filter and displays the new IPS signature filter view.

**Step 7** After an IPS signature filter is configured, all predefined signatures are contained in the signature filter by default. You can run the following commands as required to configure the filtering conditions of the signature filter to select signatures that meet the requirements.

- Run **category** { *category-name* &<1-10> | **all** }

  IPS signatures of a specified category are added to the IPS signature filter.

  By default, no IPS signatures of a specified category are added to an IPS signature filter.
- Run **protocol** { *protocol-name* &<1-10> | **all** }

  IPS signatures with a specified protocol are added to the IPS signature filter.

  By default, no protocol is specified in an IPS signature filter.
- Run **os** { **android** | **ios** | **other** | **unix-like** | **windows** } *

  IPS signatures with a specified operating system are added to the IPS signature filter.

  By default, the IPS signature filter contains signatures of all operating systems.
- Run **severity** { **high** | **information** | **low** | **medium** } *

  The threat level of IPS signatures contained in the IPS signature filter is configured.

  By default, no threat level is specified in an IPS signature filter.
- Run **target** { **both** | **client** | **server** }

  IPS signatures with a specified target are added to the IPS signature filter.

  By default, no target is specified in the IPS signature filter.

**Step 8** Run **action** { **alert** | **block** | **default** }

The action of the IPS signature filter is configured.

By default, the action of an IPS signature filter is **default**, that is, the signature filter uses the action of each signature to process packets.

**Step 9** Run **application** { *application-name* &<1-10> | **all** }

An application name in an IPS signature filter is configured.

By default, the IPS does not filter packets based on application names.

The application name specified in this command is a filtering condition in the IPS signature filter and helps filter packets of the specified application. **&<1-10>**

 Copyright © Huawei Technologies Co., Ltd. 

indicates that a maximum of 10 applications can be specified at a time. To specify more applications, repeat this command. A packet matches the filtering condition if the application type of this packet matches any of the specified applications.

**Step 10** Run **quit**

Exit from the signature filter view.

**Step 11** (Optional) Run **signature-set move** *signature-set-name1* { **before** | **after** } *signature-set-name2*

The priority of the IPS signature filter is configured.

**Step 12** (Optional) Run **exception ips-signature-id** *ips-signature-id* [ **action** { **alert** | **allow** | **block** } ]

The response method of the IPS exception signature is configured.

By default, the response method of an exception signature is **allow**.

If the response method of an IPS exception signature is different from that of the IPS profile and signature filter, the configuration of the IPS exception signature takes effect.

**Step 13** Run **quit**

Exit from the IPS profile view.

**Step 14** (Optional) Run **ips collect-attack-evidence max-session-number** *session-number* [ **signature-id** *signature-id* ]

The maximum number of attack evidence collection sessions for each IPS signature on each CPU is configured.

By default, the number of attack evidence collection sessions for each IPS signature on each CPU is 5.

You can set the maximum number of sessions in which the NGFW captures packets that match the intrusion prevention profile for each IPS signature on each CPU to collect necessary information for packet tracing, with the impact brought about by packet capture on system performance controlled to the minimum extent. When the NGFW provides multiple CPUs, the maximum number of attack evidence collection sessions for each IPS signature is the value of *session-number* multiplying the number of CPUs.

**Step 15** Run **engine configuration commit**

Configurations related to the security policy are submitted.

After creating or modifying configurations related to the security policy, the configurations do not take effect immediately. You need to run the **engine configuration commit** command to activate the configurations. Because the activation process takes a long time, you are advised to complete all configurations related to the security policy and then submit the configurations together.

**Step 16** (Optional) Run **cnc domain-filter exception domain-name** *domain-name*

An exception domain name is added.

By default, the exception domain name is not specified.

 Copyright © Huawei Technologies Co., Ltd. 

The exception domain name must be a domain name in the malicious domain name signature database. Adding any domain name that is not in the malicious domain name signature database is pointless. You can determine whether to add a malicious domain name as an exception domain name based on the threat logs. After a malicious domain name is added as an exception domain name, the device does not filter out the packets matching the exception domain name.

**Step 17** Configure protocol anomaly detection in the IPS profile view.

| Item | Command |
| --- | --- |
| Detecting whether an HTTP traffic contains the SSH traffic | **http ssh-over-http check action** { **alert** \| **block** } |
| Detecting whether an HTTP packet contains multiple **Host** fields | **http multi-host check action** { **alert** \| **block** } |
| Detecting the **X-Online-Host** field in an HTTP packet | **http x-online-host check** { **any** \| **blacklist** \| **multiple** } **action** { **alert** \| **block** }<br>**http x-online-host blacklist** *blacklist* |
| Detecting the **X-Forwarded-For** field in an HTTP packet | **http x-forwarded-for check** { **any** \| **whitelist** } **action** { **alert** \| **block** }<br>**http x-forwarded-for whitelist ipv4** *ip-address* |
| Detecting whether the protocol format of a DNS packet is abnormal | **dns malformed-packet check action** { **alert** \| **block** } |
| Detecting the query of a DNS packet | **dns request-type check** { *start-type* [ **to** *end-type* ] **action** \| **default-action** } { **alert** \| **allow** \| **block** } |

**----End**

## 7.2.8.3 Binding an IPS Profile to a Security Policy

## Context

A security policy not only forwards network traffic, but also implements integrated content security detection on network traffic. After enabling the IPS function, you need to bind an IPS profile to a security policy and apply the security policy in interzones. The device can defend against intrusions based on the security policy.

Various types of service traffic exist on the network. The device configures multiple security policies for different service traffic. Different types of profiles can be bound to a security policy at the same time. However, a security policy can only bind one profile among all profiles of the same type. To ensure that security policies are configured correctly, administrators need to complete security policy planning before configuring security policies.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

If multiple content security protection functions (such as the IPS function and URL filtering function) need to be configured concurrently, configure the IPS profile and URL filtering profile first, and run the **profile (security policy view)** command to bind the profiles to the security policy.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **security-policy** *policy-name*

A security policy is created and the security policy view is displayed.

By default, no security policy is created.

**Step 3** Run **profile ips** *ips-name* [ **acl** *acl-id* ]

An IPS profile bound to the security policy is configured.

By default, no IPS profile is bound to a security policy.

The *acl-id* has been created.

Currently, IPS only supports the binding of an ACL4, not an ACL6.

NOTE

When IPS is bound to ACL4, create bidirectional rules in the ACL to make the configuration take effect.

**----End**

## 7.2.8.4 Applying a Security Policy in Interzones

## Prerequisites

Security zones have been created and interfaces have been added to the security zones. For details, see **6.6.1 Creating a Zone and Adding Interfaces to the Zone** in "Firewall Configuration."

## Context

After the security policy configuration is complete, the security policy takes effect only when its application range is specified. The device considers that data transmission within a security zone is reliable and no security policy needs to be used. The device checks the data and carries out security policies only when the data flows from one security zone to another. When configuring the IPS service, you need to enter interzones and apply security policies that have bound IPS profiles.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall interzone** *zone-name1 zone-name2*

An interzone is created and the interzone view is displayed.

You must specify two existing security zones for the interzone.

For details about interzone, see **6.6.2 Creating an Interzone** in "Firewall Configuration."

**Step 3** Run **security-policy** *policy-name*

The security policy is applied to the interzone.

By default, no security policy is applied to an interzone.

After the security policy is applied, if no ACL is configured when an IPS profile is bound to the security policy, the device performs IPS detection for the traffic in all interzones. If an ACL is configured when an IPS profile is bound to the security policy, the device determines whether to perform IPS detection for the traffic according to ACL rules.

- If the ACL includes a permit rule, the device detects traffic that matches this rule.
- If the ACL includes a deny rule, the device does not detect traffic that matches this rule.
- If traffic does not match the ACL, the device does not detect the traffic.

**----End**

## 7.2.8.5 (Optional) Controlling the IPS Log Sending Function

## Context

When a lot of intrusion behaviors occur at a certain time, IPS triggers alarms or blocking actions frequently, and sends a large number of logs to the device in a short time. By default, the device displays logs in real time. This may refresh the screen and affect the administrator's work.

To solve the problem, you can disable the log sending function or configure the log caching function to control the IPS log sending frequency.

A maximum of 1024 logs can be recorded in the log cache. A maximum of 16 logs can be displayed each time and the displayed logs are cleared from the cache. By default, logs are displayed every minute.

NOTE

When the log cache is full, the excess logs are discarded. You can reduce the output time if the configured output time is too long and results in a full log cache.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **engine log ips enable**

The log sending function of a specified module or all modules is enabled.

By default, the system enables the log sending function of all modules.

**Step 3** Run **engine log timeout** *interval*

The log output frequency is configured.

By default, logs are displayed every minute.

**Step 4** Run **ips log merge enable**

The IPS log aggregation function is enabled.

By default, the system enables the IPS log aggregation function.

**----End**

## 7.2.8.6 Verifying the IPS Configuration

## Procedure

- Run the **display profile type ips** [ **name** *name* [ **signature-set-name** *signature-set-name* | **exception-signature-id** *exception-signature-id* ] ] command to view the current IPS profile configuration.
- Run the **display ips-signature** [ **pre-defined** [ **associated** ] | **user-defined** ] [ **application** { *application-name* | **all** } | **category** { *category-name* | **all** } | **os** { **all** | **android** | **ios** | **other** | **unix-like** | **windows** } * | **protocol** { *protocol-name* | **all** } | **severity** { **information** | **low** | **medium** | **high** }* | **state** { **disabled** | **enabled** | **retired** } | **target** { **server** | **client** | **both** } ]* command to view IPS signature information.
- Run the **display ips-signature vendor-id** *vendor-id* command to display IPS signatures of a specified vendor ID.
- Run the **display ips signature-id** *signature-id* **rule** { **name** *rule-name* | **all** } command to view user-defined IPS signature information.
- Run the **display ips signature-state** command to view the state of user-predefined IPS signature.
- Run the **display ips-signature cve-id** { *cve-id* | **year** *year* } command to display IPS signatures of a specified CVE ID.
- Run the **display cnc domain-filter exception** command to display all exception domain names.
- Run the **display security-policy** { **name** *policy-name* | **all** } command to view the security policy rule.
- Run the **display firewall zone** [ *zone-name* ] [ **interface** | **priority** ] command to view security zone information.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **display firewall interzone** [ *zone-name1 zone-name2* ] command to view interzone information.

**----End**

# 7.2.9 Maintaining IPS

## 7.2.9.1 Viewing IPS Statistics

### Context

After specified security policies are applied on interfaces, you can view IPS statistics to check detected alarm events and blocking events.

You can view statistics on the number of times that an IPS signature is matched. You can also choose to view statistics on the top 100 IPS signatures among all the IPS signatures that are matched for the most times.

### Procedure

- Run in any view:
  **display ips statistics**

  IPS statistics are displayed.
- Run in any view:
  **display ips-signature statistics** *topn-number*

  Top *topn-number* IPS signatures among all the IPS signatures that are matched for the most times are displayed.
- Run **display cnc domain-filter** { **domain** | **exception** | **domain-name** *domain-name* } **statistics**

  The domain name filtering statistics are displayed.
- Run **display cnc domain-filter domain statistics** *topn-number*

  The top *topn-number* matched malicious domain names are displayed.

**----End**

## 7.2.9.2 Clearing IPS Statistics

### Context

Before recollecting IPS statistics, run the following command in the user view to clear the existing statistics.

**NOTICE**

IPS statistics cannot be restored after they are cleared. Exercise caution when you clear the statistics.

 Copyright © Huawei Technologies Co., Ltd. 

### Procedure

**Step 1** Run **reset ips statistics**

IPS statistics are cleared.

**Step 2** Run **reset ips-signature statistics** { **signature-id** *signature-id* | **all** } { **event** | **collect-attack-evidence** | **all** }

Statistics on the number of times that an IPS signature is matched are cleared.

**Step 3** Run **reset cnc domain-filter** { **domain** | **exception** | **domain-name** *domain-name* } **statistics**

The domain name-based filtering statistics are cleared.

**----End**

## 7.2.10 Configuration Examples for IPS

### 7.2.10.1 Example for Configuring IPS to Block Intrusion Behaviors

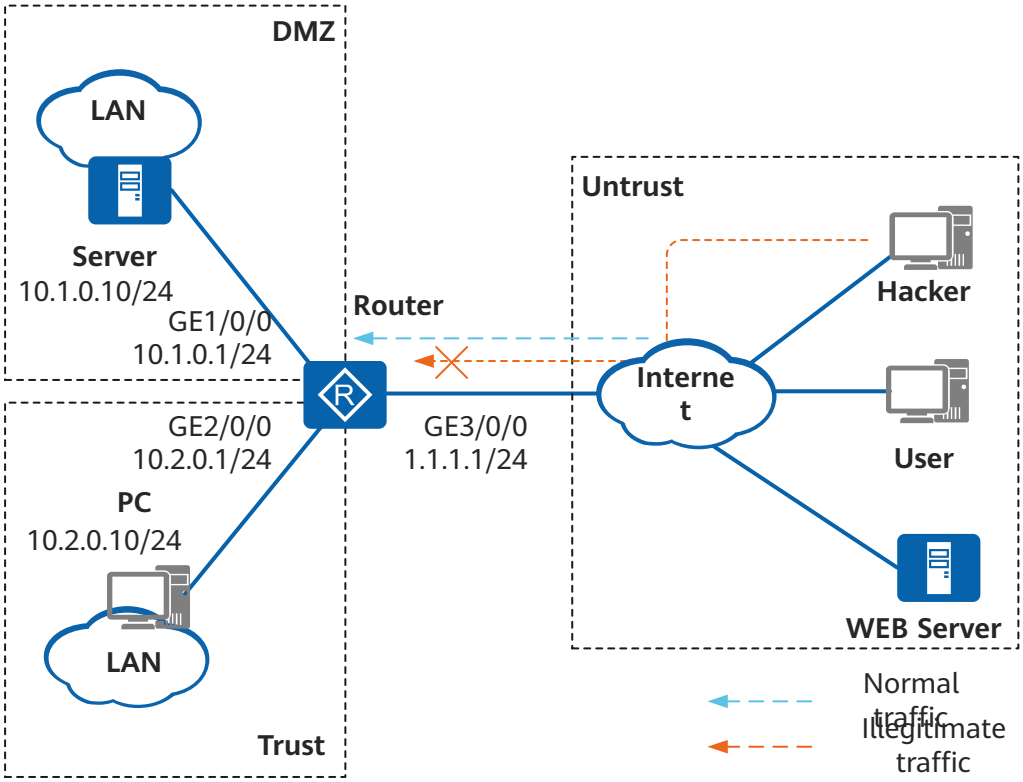
### Networking Requirements

As shown in **Figure 7-9**, an enterprise deploys a Router as the security gateway. Enterprise employees are internal users and are deployed in the Trust zone. The internal server is deployed in the demilitarized zone (DMZ).

To protect internal users and the internal server against attacks such as worms, Trojan horses, and botnets, the device needs to detect traffic between different zones and block intrusion behaviors in real time to protect the enterprise internal network security.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 7-9** Networking diagram for configuring IPS to block intrusion behaviors




## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure IP addresses and routes for interfaces to ensure connectivity.
2. Deploy the internal server, internal users and external network in the DMZ, Trust zone, and Untrust zone respectively, and monitor network traffic between different security zones.
3. For internal users, configure the IPS profile profile_ips_pc.
   a. Detect and defend against intrusion behaviors whose threat level is high.
   b. Detect and defend against intrusion behaviors whose protocol types are HTTP and FTP.
   c. Detect and defend against intrusion behaviors whose targets are clients.
4. For the internal server, configure the IPS profile profile_ips_server.
   a. Detect and defend against intrusion behaviors whose threat level is high.
   b. Detect and defend against intrusion behaviors whose protocol type is FTP.
   c. Detect and defend against intrusion behaviors whose targets are servers.
   d. Use exception signatures to block intrusion behaviors that occur frequently.
5. Configure interzones that need to be detected.


Copyright © Huawei Technologies Co., Ltd.

6. Configure two security policies policy_sec_1 and policy_sec_2, bind the IPS profiles profile_ips_pc and profile_ips_server to the two policies respectively, and detect network traffic based on the two IPS profiles.
7. Apply the security policy policy_sec_1 to the interzone between the Trust and Untrust zones. Make the security policy take effect to protect internal users against attacks from the Internet.
8. Apply the security policy policy_sec_2 to the interzone between the Untrust zone and DMZ and the interzone between the Trust zone and DMZ. Make the security policy take effect to protect the internal server against attacks from internal users and the Internet.

## Procedure

**Step 1** Configure security zones and interzones on the Router.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] engine enable
[Router] firewall zone DMZ
[Router-zone-DMZ] priority 14
[Router-zone-DMZ] quit
[Router] firewall zone Trust
[Router-zone-Trust] priority 13
[Router-zone-Trust] quit
[Router] firewall zone Untrust
[Router-zone-Untrust] priority 1
[Router-zone-Untrust] quit
[Router] firewall interzone Trust Untrust
[Router-interzone-Trust-Untrust] quit
[Router] firewall interzone DMZ Trust
[Router-interzone-DMZ-Trust] quit
[Router] firewall interzone DMZ Untrust
[Router-interzone-DMZ-Untrust] quit
```

**Step 2** Configure IP addresses for interfaces on the Router and add the interfaces to security zones.

```
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 10.1.0.1 24
[Router-GigabitEthernet1/0/0] zone DMZ
[Router-GigabitEthernet1/0/0] quit
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] ip address 10.2.0.1 24
[Router-GigabitEthernet2/0/0] zone Trust
[Router-GigabitEthernet2/0/0] quit
[Router] interface gigabitethernet 3/0/0
[Router-GigabitEthernet3/0/0] ip address 1.1.1.1 24
[Router-GigabitEthernet3/0/0] zone Untrust
[Router-GigabitEthernet3/0/0] quit
```

**Step 3** Configure the IPS profile profile_ips_pc to protect internal users. Configure signature filters to meet security requirements.

```
[Router] profile type ips name profile_ips_pc
[Router-profile-ips-profile_ips_pc] signature-set name filter1
[Router-profile-ips-profile_ips_pc-sigset-filter1] target client
[Router-profile-ips-profile_ips_pc-sigset-filter1] severity high
[Router-profile-ips-profile_ips_pc-sigset-filter1] protocol HTTP FTP
[Router-profile-ips-profile_ips_pc-sigset-filter1] action default
[Router-profile-ips-profile_ips_pc-sigset-filter1] quit
[Router-profile-ips-profile_ips_pc] quit
```

**Step 4** Configure the IPS profile profile_ips_server to protect the internal server. It is observed in logs that a type of attacks occurs frequently. The attacks match a signature whose ID is 74320. All attacks of this type need to be blocked.

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router] profile type ips name profile_ips_server
[Router-profile-ips-profile_ips_server] signature-set name filter1
[Router-profile-ips-profile_ips_server-sigset-filter1] target server
[Router-profile-ips-profile_ips_server-sigset-filter1] severity high
[Router-profile-ips-profile_ips_server-sigset-filter1] protocol FTP
[Router-profile-ips-profile_ips_server-sigset-filter1] action default
[Router-profile-ips-profile_ips_server-sigset-filter1] quit
[Router-profile-ips-profile_ips_server] exception ips-signature-id 74320 action block
[Router-profile-ips-profile_ips_server] quit
[Router] engine configuration commit
```

**Step 5** Create a security policy named policy_sec_1 and bind the IPS profile profile_ips_pc to the security policy.

```
[Router] security-policy policy_sec_1
[Router-security-policy-policy_sec_1] profile ips profile_ips_pc
[Router-security-policy-policy_sec_1] quit
```

**Step 6** Create a security policy named policy_sec_2 and bind the IPS profile profile_ips_server to the security policy.

```
[Router] security-policy policy_sec_2
[Router-security-policy-policy_sec_2] profile ips profile_ips_server
[Router-security-policy-policy_sec_2] quit
```

**Step 7** Apply the security policy policy_sec_1 to the interzone between the Trust and Untrust zones. Make the security policy take effect to protect internal users against attacks from the Internet.

```
[Router] firewall interzone Trust Untrust
[Router-interzone-Trust-Untrust] security-policy policy_sec_1
[Router-interzone-Trust-Untrust] quit
```

**Step 8** Apply the security policy policy_sec_2 to the interzone between the DMZ and Untrust zone and the interzone between the DMZ and Trust zone. Make the security policy take effect to protect the internal server against attacks from internal users and the Internet.

```
[Router] firewall interzone DMZ Untrust
[Router-interzone-DMZ-Untrust] security-policy policy_sec_2
[Router-interzone-DMZ-Untrust] quit
[Router] firewall interzone DMZ Trust
[Router-interzone-DMZ-Trust] security-policy policy_sec_2
[Router-interzone-DMZ-Trust] quit
```

**Step 9** Verify the configuration.

On the Router, run the **display security-policy name** *policy-name* command to view the security policy.

```
<Huawei> display security-policy name policy_sec_1
  Policy-name: policy_sec_1
  Policy-ID: 4
   IPS: profile_ips_pc
   URLF: -
   ACL: 0
  Reference-Num: 1
```

On the Router, run the **display firewall interzone** *zone-name1 zone-name2* command. The result is as follows:

```
<Huawei> display firewall interzone Trust Untrust
interzone Trust Untrust
 firewall disable
 security-policy policy_sec_1
 packet-filter default deny inbound
 packet-filter default permit outbound
```

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## Configuration File

Configuration file of the Router

```
#
 sysname Router
#
 engine enable
#
profile type ips name profile_ips_pc
 signature-set name filter1
  target client
  severity high
  protocol HTTP FTP
#
profile type ips name profile_ips_server
 signature-set name filter1
  target server
  severity high
  protocol FTP
 exception ips-signature-id 74320 action block
#
security-policy policy_sec_1
  profile ips profile_ips_pc
security-policy policy_sec_2
  profile ips profile_ips_server
#
firewall zone Untrust
 priority 1
#
firewall zone DMZ
 priority 14
#
firewall zone Trust
 priority 13
#
firewall interzone Trust Untrust
 security-policy policy_sec_1
#
firewall interzone DMZ Trust
 security-policy policy_sec_2
#
firewall interzone DMZ Untrust
 security-policy policy_sec_2
#
interface GigabitEthernet1/0/0
 ip address 10.1.0.1 255.255.255.0
 zone DMZ
#
interface GigabitEthernet2/0/0
 ip address 10.2.0.1 255.255.255.0
 zone Trust
#
interface GigabitEthernet3/0/0
 ip address 1.1.1.1 255.255.255.0
 zone Untrust
#
return
```

# 7.3 URL Filtering Configuration

Uniform Resource Locator (URL) filtering regulates online behaviors by controlling which URLs users can access.

 Copyright © Huawei Technologies Co., Ltd. 

# 7.3.1 Overview of URL Filtering

With rapid development of Internet applications and popularity of computer networks, acquisition, sharing, and dissemination of information has become more widespread than ever, which brings unprecedented threats to enterprises:

- Visiting non-work-related websites during working hours reduces work efficiency.
- Visiting illegitimate or malicious websites may result in threats such as worms, viruses, and Trojan horses.

Uniform Resource Locator (URL) filtering regulates online behaviors by controlling which URLs users can access.

# 7.3.2 Understanding URL Filtering

URL filtering allows the device to accurately manage online behaviors of users who access network resources through HTTP.

## 7.3.2.1 URL Matching Mode

After the device receives an HTTP request, it parses the HTTP request and uses a specified method to match the HTTP request with a URL. If the URL is matched, the device processes the HTTP request according to the action taken for the URL.

A URL is the address of a web page or an accessible resource on the Internet.

The standard format of a URL is protocol://hostname[:port]/path[?query]. **Table 7-4** describes the fields.

**Table 7-4** URL fields

| Field | Description |
| --- | --- |
| protocol | Used application protocol. HTTP is often used. |
| hostname | Domain name or IP address of the web server. |
| :port | (Optional) Communication port. Application protocols have default ports. For example, the default port for HTTP is 80. If the server uses the default port, you do not need to configure the port number in a URL filtering rule. If the server uses a non-default port, the port number is mandatory in a URL filtering rule. |
| path | Directory or file path on the web server. The path is a character string that can be separated by slashes (/). |
| ?query | (Optional) This field is used to transmit parameters to dynamic web pages. |

URL matching modes include prefix matching, suffix matching, keyword matching, and exact matching. **Table 7-5** describes the four matching modes.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 7-5** URL matching modes

| Matching Mode | Function | Example | Result |
| --- | --- | --- | --- |
| Prefix matching | Matches URLs that start with a specified character string. | www.test.com* | All URLs that start with **www.test.com** are matched, for example, **www.test.com** and **www.test.com/solutions.do**. |
| Suffix matching | Matches URLs that end with a specified character string. | *aspx | All URLs that end with **aspx** are matched, for example, **www.test.com/news/solutions.aspx** and **www.test.com/it/price.aspx**. |
| Keyword matching | Matches URLs that include a specified character string. | *sport* | All URLs that include **sport** or **ab*cd** are matched, for example, **sports.test.com/news/solutions.aspx**, **sports.test.com/it/**. |

 Copyright © Huawei Technologies Co., Ltd. 

| Matching Mode | Function | Example | Result |
| --- | --- | --- | --- |
| Exact matching | First checks whether the URL matches the specified character string. If no, delete the last directory of the URL and check again. If the URL is still not matched, delete the second last directory and check again until the domain name can match a specific character string. | www.example.com | Based on matching rules, the following URLs match www.example.com:<br>• www.example.com<br>• www.example.com/news<br>• www.example.com/news/en/<br>The following URLs will not match www.example.com:<br>• www.example.com.cn/news<br>• www.example.org/news/ |

The priorities of URL matching modes are as follows:

Exact matching > suffix matching > prefix matching > keyword matching

For example, URL **www.example.com/news** first matches **www.example.com/news** in the following prefix matching rules:

- Exact matching: www.example.com/news
- Prefix matching: www.example.com/*
- Keyword matching: *example*

In the same matching mode, a long matching rule is assigned a higher priority than a short one. For example, URL **www.example.com/news/index.html** first matches **www.example.com/news/*** in the following prefix matching rules:

- www.example.com/news/*
- www.example.com/*

If the matching rules have the same length in the same matching mode, the action mode is used to determine the rule to which a rule matches. As shown in **Table 7-6**, the two URL rules are in **keyword matching** mode and have the same length (4). As for URL **www.example.com/welcome.html**:

- If the action mode is **strict mode**, the URL will match the category with a stricter action. In this example, the URL matches category B whose action is block.


Copyright © Huawei Technologies Co., Ltd.

- If the action mode is **loose mode**, the URL will match the category with a looser action. In this example, the URL matches category A whose action is permit.

**Table 7-6** Action mode

| Item | URL Category | Control Action |
| --- | --- | --- |
| *.com* | URL category A | Permit |
| *html* | URL category B | Block |

NOTE

- In all of the matching modes, the device removes **http://** from the beginning of the entered character string. In the exact matching mode, the device adds a slash (/) at the end of character strings that do not contain any slashes (/) after the **hostname**.
- URLs are case insensitive.
- This section mainly describes URL matching details. For details on URL control actions, see **7.3.2.2 Working Mechanism of URL Filtering**.

## 7.3.2.2 Working Mechanism of URL Filtering

When an HTTP request matches a URL, the device processes the HTTP request according to the **URL Filtering Mode** and **URL Filtering Process**.

## URL Filtering Mode

The device provides URL filtering based on the blacklist, whitelist, and URL category:

- Blacklist and whitelist: The device filters received HTTP requests according to the manually configured **URL Whitelist** or **URL Blacklist**.
- URL category: After receiving an HTTP request, the device queries the URL category in **URL Category**. After the URL category is found, the device processes the HTTP request according to the **Action** configured for the URL category.

The blacklist, whitelist, URL category, and action are described as follows:

- **URL whitelist**: Enterprises can add URLs of network resources that employees are allowed to access to a URL whitelist. When URLs in HTTP requests match the URL whitelist, the device allows the HTTP requests to pass through.
- **URL blacklist**: Enterprises can add URLs of network resources that employees are not allowed to access to a URL blacklist. When URLs in HTTP requests match the URL blacklist, the device rejects the HTTP requests and displays the blacklist blocking page.
- **URL category**: URL categories fall into user-defined and predefined URL categories.
  - User-defined categories are configured and maintained by administrators and enable more refined control over URLs than predefined categories.

 Copyright © Huawei Technologies Co., Ltd. 

  - Predefined categories contain commonly used URLs. Predefined categories enable administrators to easily control accessible and inaccessible URL categories.

    Predefined URL category query has one mode:

    - Local URL filtering: A predefined URL category database is loaded to the local cache of the device before delivery. You can use this database if there is no special requirement. When the predefined URL category database fails to be loaded or the security service center updates the predefined URL category database, manually load the new predefined URL category to the local cache. After obtaining the URL information, the device queries the category matching the URL in the cache first. If a category is found, the device takes the action in the URL filtering configuration file. If no matching category is found, the device takes the default action.

- **Action**: After the device finds a URL category matching an HTTP request, it processes the HTTP request according to the action taken for the URL category. Currently, the device supports the following actions:
  - **allow**: The device does not process the HTTP request, and allows the HTTP request to pass through.
  - **alert**: The device allows the HTTP request to pass through and generates a log.
  - **block**: The device rejects the HTTP request and generates a log. In addition, the device displays the blocking page.

If a URL belongs to multiple categories, the NGFW takes an action based on the action mode.

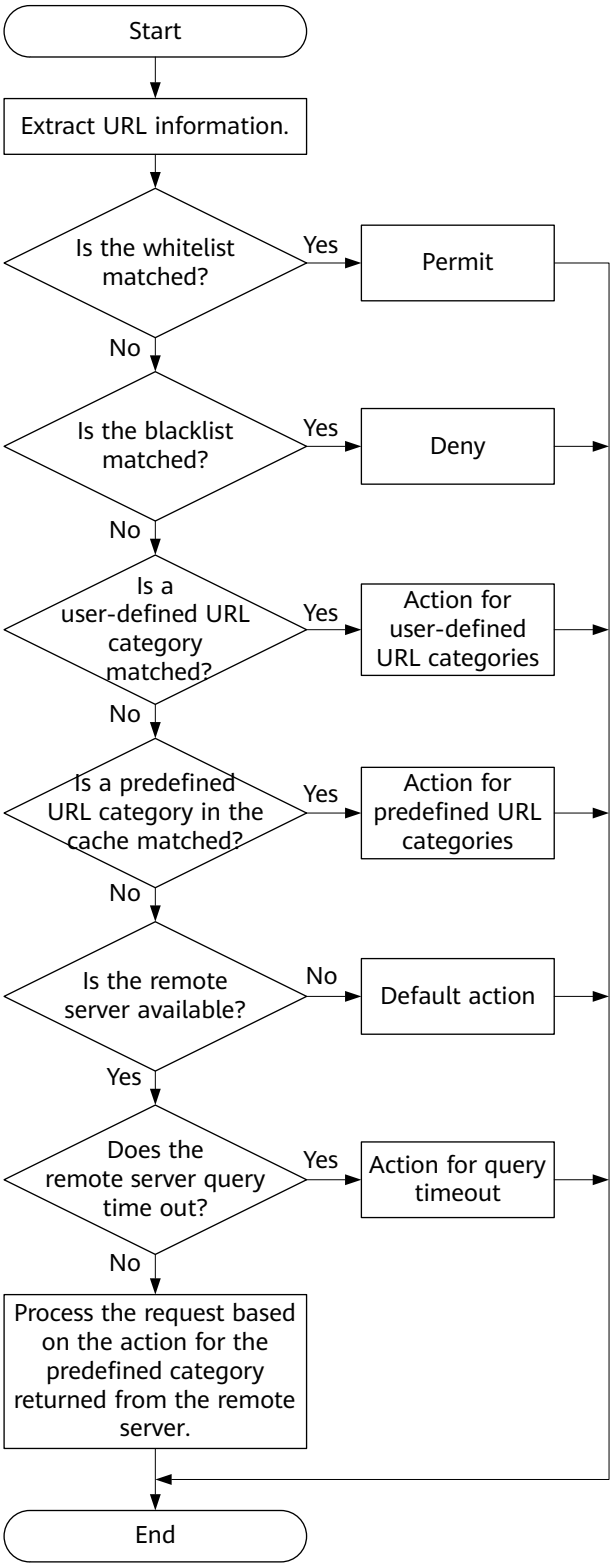
- Strict: The NGFW takes the strictest action among all matched categories. For example, a URL belongs to two categories, and the actions are **Alert** and **Block**. In this case, the NGFW takes the **Block** action.
- Loose: The NGFW takes the loosest action among all matched categories. For example, a URL belongs to two categories, and the actions are **Alert** and **Block**. In this case, the NGFW takes the **Alert** action.

## URL Filtering Process

URL filtering enables the device to filter HTTP requests passing through the device. **Figure 7-10** shows the URL filtering process.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 7-10** URL filtering process




If a user accesses a network resource using HTTP through the device, the device applies the filter as follows:

1. A user initiates a URL access request. If the data flow matches a security policy, and the action of the policy is permit, the system implements URL filtering.
2. The device matches the URL with the whitelist.
   - If the URL matches the whitelist, the device permits the URL access request.
   - If the URL does not match the whitelist, the device proceeds to the next step.
3. The device matches the URL with the blacklist.
   - If URL information matches the blacklist, the device blocks the URL access request.
   - If the URL does not match the blacklist, the device proceeds to the next step.
4. The device matches the URL with user-defined categories.
   - If the URL matches a user-defined category, the device processes the request based on the action for this user-defined category.

     NOTE

     URLs added to predefined categories are still considered user-defined URLs.
   - If the URL does not match user-defined categories, the device proceeds to the next step.
5. The device matches the URL with predefined categories in the cache.
   - If a predefined category is matched, the device processes the request based on the action for this predefined category.
   - If no predefined category is matched, the device processes the request based on the default action.

# 7.3.3 Applicable Scenarios for URL Filtering

## 7.3.3.1 Using URL Filtering to Regulate Online Behaviors

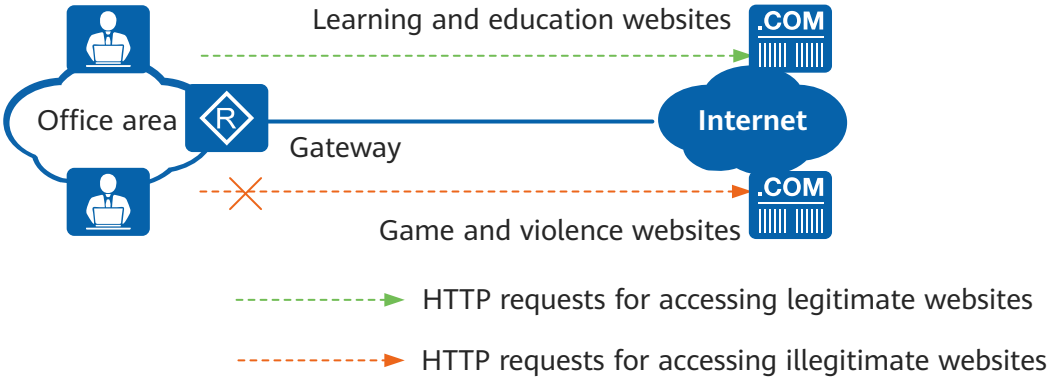
URL filtering is often deployed on an enterprise gateway to accurately manage online behaviors of users who access network resources through HTTP/HTTPS.

As shown in **Figure 7-11**, the device is deployed at the network edge and works as the enterprise gateway. When enterprise users send HTTP/HTTPS requests, the device uses URL filtering to control websites that enterprise users access. For example:

- The device allows enterprise users to access learning and education websites.
- The device prevents enterprise users from accessing game and violence websites.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 7-11** Networking of URL filtering




# 7.3.4 Licensing Requirements and Limitations for URL Filtering

## Involved Network Elements

Other network elements are not required.

## Licensing Requirements

For URL filtering-capable devices, their licensing requirements for the URL filtering function are as follows:

- AR100&AR120 series: URL filtering is a basic feature of the device and is not under license control.
- AR150&AR160&AR200&AR1200&AR2200&AR3200 series: by default, this function is disabled on a new device. To use the URL filtering function, apply for and purchase the following license from the Huawei local office.
  - AR150&AR160&AR200 series: AR150&160&200 Value-Added Security Package
  - AR1200 series: AR1200 Value-Added Security Package
  - AR2200 series: AR2200 Value-Added Security Package
  - AR3200 series: AR3200 Value-Added Security Package

## Feature Limitations

When deploying URL filtering on the router, pay attention to the following:

- The device supports URL filtering that involves personal communication information collection or storage. Huawei will not collect or save user communication information independently. You must use the features in compliance with applicable laws and regulations. Ensure that your customers' privacy is protected when you are collecting or saving communication information.
- URL filtering applies only to HTTP or HTTPS URL requests. To filter HTTPS URL requests, you also need to configure encrypted traffic filtering function.

 Copyright © Huawei Technologies Co., Ltd. 

However, the URL filtering implemented by the encrypted traffic filtering function is at the domain name level, which is not accurate enough. It obtains the domain name of the website that a user accesses from the Server Name Indication (SNI) field in the client's Client Hello packet and the Common Name (CN) and Subject Alternative Name (SAN) fields in the server's Certificate packet. Before using the encrypted traffic filtering function to implement HTTPS URL filtering, read the following restrictions:

- When a browser has a proxy server, the domain name extracted by the router from the SNI field in the client's Client Hello packet and the CN and SAN fields in the server's Certificate packet may be different from the actual domain name of the website. If this happens, URL filtering does not take effect. For example, when a user uses the UC browser on a mobile phone to access Youku, URL filtering does not take effect. To resolve this issue, disable the cloud acceleration function of the UC browser on the mobile phone.
- If some browsers use proprietary protocols to transmit data, URL filtering may not take effect. For example, Google Chrome uses the proprietary protocol Quick UDP Internet Connection (QUIC) for data transmission by default. This protocol uses a dedicated encryption mode that the router cannot decrypt. As a result, URL filtering cannot filter HTTPS websites accessed through Google Chrome.
- When a website server provides services for multiple domain names using the same IP address, the SNI field may contain multiple domain names. If only one domain name is configured in the URL filtering blacklist, not all traffic from this website cannot be blocked. For example, when a user accesses **www.example.com** through HTTPS, the website may have multiple domain names, such as **1.example.com** and **2.example.com**. If only **1.example.com** is configured in the URL filtering blacklist, not all traffic of this website cannot be blocked. To resolve this issue, configure level-1 domain name ***.example.com** in the blacklist.
- When a certificate contains multiple URLs (that is, multiple websites use one certificate), the SAN field may contain multiple URLs. If one URL is blocked, the traffic from this URL is blocked and other URLs cannot be accessed.
- If the domain name of a website is added to the URL filtering whitelist, not all embedded pages of the website can be accessed. For example, if only **www.example.com** is added to the whitelist, the embedded pages whose domain names are not **www.example.com** cannot be accessed.
- Encrypted traffic filtering implements URL filtering through SSL handshake packets. The client does not initiate an HTTP request. Therefore, sending URL push information is not supported.

- The following product models support URL filtering function:
  - AR100&AR120&AR150&AR160&AR200&AR3200 series: All models.
  - AR1200 series: AR1220C, AR1220-8GE, AR1220E, AR1220EV, and AR1220EVW.
  - AR2200 series: all models except AR2201-48FE, AR2202-48FE, and AR2204.

 Copyright © Huawei Technologies Co., Ltd. 

# 7.3.5 Enabling the Deep Security Function

## Context

To use the IPS or URL filtering function, you need to purchase a license and run the **engine enable** command to enable the deep security function.

To disable deep security, run the **undo engine enable** command, and restart the device. After the device restarts, the deep security configurations are deleted.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **engine enable**

The deep security function is enabled.

By default, the system disables the deep security function.

NOTE

If the **engine enable** command is executed for the first time, you need to run the **update restore sdb-default** command to manually load the signature file.

**----End**

# 7.3.6 Configuring URL Filtering

## 7.3.6.1 Configuring a URL Filtering Profile

## Context

To accurately manage online behaviors of users, a URL filtering profile defines the predefined URL categories, user-defined URL categories, blacklist, and whitelist to control URLs. The device filters the content of an HTTP request, extracts the URL, and matches the URL with the whitelist, blacklist, user-defined URL category, or predefined URL category. If the URL is matched, the device processes the HTTP request according to the configured action.

The whitelist, blacklist, and predefined and user-defined URL categories are applicable to the following scenarios:

- A predefined URL category is used to define many common websites accessed by enterprise employees.
- A user-defined URL category is used to define new websites not in the predefined URL category and customized websites meeting special requirements.
- A blacklist is used to define websites that enterprise employees are not allowed to access.
- A whitelist is used to define websites that enterprise employees are allowed to access.

 Copyright © Huawei Technologies Co., Ltd. 

Generally, a predefined URL category is mandatory, and the user-defined URL category, whitelist, and blacklist are optional.

If duplicate rules are configured for the predefined URL category, user-defined URL category, blacklist, or whitelist, they are recorded as only one rule.

## Procedure

- Configuring a URL filtering profile that defines a predefined URL category
  a. (Optional) Configure a predefined URL category.
     i. Run **system-view**

        The system view is displayed.
     ii. Run **url-filter category pre-defined subcategory-id** *subcategory-id*

        The predefined URL subcategory view is displayed.

        NOTE

        During factory delivery, there is a predefined URL category database. When the predefined URL category database fails to be loaded or the security service center updates the predefined URL category database, run the **import url-sdb file** *filename* command to import a URL category database.
     iii. Run **add** { **url** *url-text* | **host** *host-text* }

        A URL or domain name rule is added to a predefined category.

        By default, no URL or domain name rule is configured for a predefined URL subcategory.
     iv. Run **quit**

        Return to the system view.
  b. Configure an action for the predefined URL category.
     i. Run the following commands as required.
        - Run the **profile type url-filter name** *name* command to create a URL filtering profile and enter the URL filtering profile view if no URL filtering profile exists on the device.
        - To speed up configuration of a URL filtering profile, run the **profile type url-filter copy** *old-name* [ *new-name* ] command to create a URL filtering profile by copying an existing one and enter the view of the created URL filtering profile if a URL filtering profile exists on the device.

        By default, no URL filtering profile is configured.
     ii. (Optional) Run **category action mode** { **strict** | **loose** }

        The action mode of URL filtering is configured.

        By default, the action mode of URL filtering is the strict mode.
     iii. (Optional) Run **description** *description*

        The description is configured for the URL filtering profile.

        By default, no description is configured for a URL filtering profile.
     iv. Run **category pre-defined control-level** { **high** | **low** | **medium** }

        A control level is configured for the predefined URL category.

        By default, the control level of a predefined URL category is **low**.

 Copyright © Huawei Technologies Co., Ltd. 

The system defines **high**, **medium**, and **low** control levels, and configures an action for all predefined URL categories according to each control level. A high control level indicates a strict action for URL categories, for example, the device blocks HTTP requests matching porn, P2P download, and video categories. A low control level indicates a loose action for URL categories, for example, the device blocks HTTP requests matching porn categories only.

v. Run **category pre-defined** [ **category-id** *category-id* | **subcategory-id** *subcategory-id* ] **action** { **allow** | **block** | **alert** }

An action is configured for the predefined URL category.

By default, the action in a predefined URL category is **allow**.

vi. (Optional) Run **default action (URL filtering profile view)** { **allow** | **block** | **alert** }

The default action is configured for the URL filtering profile.

By default, the default action in a predefined URL category is **allow**.

vii. (Optional) Run **https-filter enable**

Enable the encrypted traffic filtering function.

By default, the function is disabled.

viii. Run **quit**

Return to the system view.

ix. Run **engine configuration commit**

The URL filtering configuration is committed.

After the security policy configurations including intrusion defense and URL filtering configurations are created or modified, you must run the **engine configuration commit** command to commit the configurations to make the configurations take effect. Committing the configurations takes a long period of time. It is recommended that you commit the configurations after modifying all security policy configurations.

- Configuring a URL filtering profile that defines a user-defined URL category

  a. Configure a user-defined URL category.

     i. Run **system-view**

     The system view is displayed.

     ii. Run the following commands as required.

     - Run the **url-filter category user-defined name** *category-name* command to create a user-defined URL category and enter the view of the user-defined URL category.
     - Run the **url-filter category pre-defined copy** *subcategory-id new-name* command to create a user-defined URL category by copying an existing predefined URL category and enter the view of the created user-defined URL category if the content of the new user-defined URL category is similar to the content of the existing predefined URL category.
     - Run the **url-filter category user-defined copy** *old-name* [ *new-name* ] command to create a user-defined URL category by copying an existing one and enter the view of the created user-

 Copyright © Huawei Technologies Co., Ltd. 

defined URL category if the content of the new user-defined URL category is similar to the content of the existing one.

By default, no user-defined URL category exists.

iii. (Optional) Run **description** *description*

The description is configured for the user-defined URL category.

By default, no description is configured for a user-defined URL category.

iv. Run **add** { **url** *url-text* | **host** *host-text* }

A URL or domain name rule is added to the user-defined category.

By default, no URL or domain name rule is added to the user-defined category.

v. Run **quit**

Return to the system view.

b. Configure an action for the user-defined URL category.

i. Run the following commands as required.

- Run the **profile type url-filter name** *name* command to create a URL filtering profile and enter the URL filtering profile view if no URL filtering profile exists on the device.
- To speed up configuration of a URL filtering profile, run the **profile type url-filter copy** *old-name* [ *new-name* ] command to create a URL filtering profile by copying an existing one and enter the view of the created URL filtering profile if a URL filtering profile exists on the device.

By default, no URL filtering profile is configured.

ii. (Optional) Run **description** *description*

The description is configured for the URL filtering profile.

By default, no description is configured for a URL filtering profile.

iii. Run **category user-defined** [ **name** *category-name* ] **action** { **allow** | **block** | **alert** }

An action is configured for the user-defined URL category.

By default, the action in a user-defined URL category is **allow**.

iv. (Optional) Run **https-filter enable**

Enable the encrypted traffic filtering function.

By default, the function is disabled.

v. Run **quit**

Return to the system view.

vi. Run **engine configuration commit**

The URL filtering configuration is committed.

- Configuring a URL filtering profile that defines the blacklist and whitelist

a. Run **system-view**

The system view is displayed.

b. Run the following commands as required.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **profile type url-filter name** *name* command to create a URL filtering profile and enter the URL filtering profile view if no URL filtering profile exists on the device.
- To speed up configuration of a URL filtering profile, run the **profile type url-filter copy** *old-name* [ *new-name* ] command to create a URL filtering profile by copying an existing one and enter the view of the created URL filtering profile if a URL filtering profile exists on the device.

By default, no URL filtering profile is configured.

c. (Optional) Run **description** *description*

The description is configured for the URL filtering profile.

By default, no description is configured for a URL filtering profile.

d. (Optional) Run **https-filter enable**

Enable the encrypted traffic filtering function.

By default, the function is disabled.

e. Run the following commands as required.

- Run **add whitelist** { **url** *url-text* | **host** *host-text* }

  A whitelist rule is added to the URL filtering profile.
- Run **add blacklist** { **url** *url-text* | **host** *host-text* }

  A blacklist rule is added to the URL filtering profile.

f. Run **add referer-host** *host-text*

Add a referer-host rule to the URL filtering profile.

The referer field in an HTTP request will be matched with the referer-host rule. If a match is found, the URL request is allowed. If the referer field in the HTTP request does not match the configured referer-host rule, the user can determine whether to match the referer field with all whitelist rules.

- When the function of matching the referer field in a URL request with whitelist rules is enabled, the referer field will be matched with all whitelist rules. If a match is found, the URL request is allowed.
- When the function of matching the referer field with whitelist rules is disabled, the referer field will not be matched with all whitelist rules.

By default, the function of matching the referer field in a URL request with whitelist rules is enabled. If the function is disabled, you can run the **undo referer-filter whitelist-all enable** command to disable it. If referer-host is not configured and the function of matching the referer field with the whitelist is enabled, the Router matches the referer field in the HTTP request with all whitelist rules. If the referer field matches a whitelist rule, the URL request is allowed.

g. Run **quit**

Return to the system view.

 Copyright © Huawei Technologies Co., Ltd. 

h. Run **engine configuration commit**

The URL filtering configuration is committed.

**----End**

## Follow-up Procedure

After the URL filtering profile is configured, you can rename the user-defined URL category or URL filtering profile to facilitate management.

- Run the **rename** *new-name* command in the URL filtering profile view to rename an existing URL filtering profile and enter the view of the new profile.
- Run the **rename** *new-name* command in the URL filtering profile view to rename an existing user-defined URL category and enter the view of the new user-defined URL category.

## 7.3.6.2 Binding a URL Filtering Profile to a Security Policy

## Prerequisites

If an ACL needs to be referenced when you bind a URL filtering profile to a security policy, ensure that the ACL has been created using the acl (system view) command.

## Context

The device uses a security policy to implement integrated detection of content security. After a URL filtering profile is configured, you need to bind the URL filtering profile to a security policy and apply the security policy to an interzone so that the device can regulate online behaviors according to the security policy.

There are various types of service traffic on a network and multiple security policies are configured on the device. A security policy can be bound to profiles of different types and only one profile of the same type.

NOTE

To configure various content security protection functions (for example, URL filtering and **IPS** need to be configured simultaneously), configure a URL filtering profile and IPS profile, and run the profile (security policy view) command to bind the URL filtering profile and IPS profile to a security policy.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **security-policy** *policy-name*

A security policy is created and the security policy view is displayed.

By default, no security policy is created.

**Step 3** Run **profile urlf** *urlf-name* [ **acl** *acl-id* ]

 Copyright © Huawei Technologies Co., Ltd. 

A URL filtering profile is bound to the security policy.

By default, no URL filtering profile is bound to a security policy.

NOTE

When URL filtering profile is bound to ACL4, create bidirectional rules in the ACL to make the configuration take effect.

**----End**

## 7.3.6.3 Binding the Security Policy to an Interzone

### Prerequisites

- An interzone has been created and an interface has been added to the interzone according to **6.6.1 Creating a Zone and Adding Interfaces to the Zone**.
- An interzone has been created according to **6.6.2 Creating an Interzone**.
- A security policy has been configured according to **7.3.6.2 Binding a URL Filtering Profile to a Security Policy**.

### Context

URL filtering takes effect only when the range that the URL filtering rule is applied is specified.

Security check is triggered only when data flows between different interzones. To make URL filtering take effect, bind a security policy to an interzone.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **firewall interzone** *zone-name1 zone-name2*

An interzone is created and the interzone view is displayed.

By default, no interzone is created.

You must specify two existing zones for the interzone.

**Step 3** Run **security-policy** *policy-name*

The security policy is bound to the interzone.

By default, no security policy is bound to an interzone.

If no ACL is configured when a URL filtering profile is bound to a security policy, the device performs URL filtering for traffic in all interzones. If an ACL is configured when a URL filtering profile is bound to a security policy, the device determines whether to perform URL filtering for traffic according to the ACL rule:

- If the ACL rule defines a permit clause, the device detects traffic matching the ACL rule.

 Copyright © Huawei Technologies Co., Ltd. 

- If the ACL rule defines a deny clause, the device does not detect traffic matching the ACL rule.
- If traffic does not match the ACL, the device does not detect the traffic.

**Step 4** Run **quit**

Return to the system view.

**----End**

## 7.3.6.4 (Optional) Configuring the Device to Control generating of URL Filtering Logs

## Context

If URL requests of many users in a period of time match the URL blacklist, user-defined URL category, or predefined URL category, the URL filtering module reports many logs to the device in a short time. If the device outputs logs in real time, the administrator has to flood the screen.

To address this issue, configure the log cache function to control the frequency in generating URL filtering logs, or disable the URL filtering module from generating logs so that the URL filtering module does not report logs.

## Procedure

- Configuring the log cache function
  a. Run **system-view**

     The system view is displayed.
  b. Run **engine log url-filter enable**

     The URL filtering module is enabled to generate logs.

     By default, the URL filtering module is enabled to generate logs.
  c. Run **engine log timeout** *time*

     The period for caching logs is set.

     By default, the period for caching logs is 1 minute.
- Disabling the URL filtering module from generating logs
  a. Run **system-view**

     The system view is displayed.
  b. Run **undo engine log url-filter enable**

     The URL filtering module is disabled from generating logs.

     By default, the URL filtering module is enabled to generate logs.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## 7.3.6.5 (Optional) Configuring user group-based URL Filtering

### Context

The Web management system supports user group management and user group-based URL filtering. Managing users' online behavior can control the network access rights of users. You can bind a URL filtering profile to a user group and enable URL filtering to manage online behavior of all users in the user group.

NOTE

Only the models that support the web system of the EasyOperation edition support this configuration. For details, see EasyOperation Edition.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **profile type url-filter name** *name*

A URL filtering profile is created and its view is displayed.

By default, no URL filtering profile is configured.

**Step 3** Run **quit**

Return to the system view.

**Step 4** Run **web**

The web view is displayed.

**Step 5** Run **user-set** *user-set-name*

A web user group is created and the web user group view is displayed, or the view of an existing web user group is displayed.

By default, the device contains two web user groups named **VIP** and **Default**.

**Step 6** Run **quit**

Return to the web view.

**Step 7** Run **web-url-filter user-set** *user-set-name* **profile** *profile-name* [ **time-range** *time-range-name* ] [ **description** *description-text* ]

User group-based URL filtering is enabled.

By default, user group-based URL filtering is disabled.

**Step 8** Run **quit**

Return to the system view.

**----End**

## 7.3.6.6 Verifying the URL Filtering Configuration

 Copyright © Huawei Technologies Co., Ltd. 

### Prerequisites

The URL filtering configuration is complete.

### Procedure

- Run the **display url-filter category pre-defined** [ **category-id** *category-id* | **subcategory-id** *subcategory-id* | **url** *url-text* | **host** *host-text* ] command to check predefined URL category information.
- Run the **display url-filter category user-defined** [ **name** *category-name* | **url** *url-text* | **host** *host-text* ] command to check user-defined URL category information.
- Run the **display profile type url-filter**or **display profile type url-filter name** *name* [ **blacklist** [ **url** *url-text* | **host** *host-text* ] | **whitelist** [ **url** *url-text* | **host** *host-text* ] | **pre-defined** [ **category-id** *category-id* | **subcategory-id** *subcategory-id* ] | **user-defined** [ **name** *category-name* ] ] command to check URL filtering profile information.

**----End**

## 7.3.7 Maintaining URL Filtering

### 7.3.7.1 Displaying URL Filtering Statistics

### Context

To view information such as the numbers of forwarded and rejected HTTP requests and the number of times a URL category is matched after URL filtering is enabled, run the **display url-filter statistics** command to view URL filtering statistics.

### Procedure

- Run the **display url-filter statistics** command to view URL filtering statistics.

**----End**

### 7.3.7.2 Clearing URL Filtering Statistics

### Context

Before recollecting URL filtering statistics, run the **reset url-filter statistics** command to clear existing URL filtering statistics.

**NOTICE**

Cleared URL filtering statistics cannot be restored. Exercise caution when running the **reset url-filter statistics** command.

 Copyright © Huawei Technologies Co., Ltd. 

### Procedure

- Run the **reset url-filter statistics** { **blacklist** | **whitelist** | **category** [ **user-defined** | **pre-defined** ] | **all** } command to clear URL filtering statistics.

**----End**

## 7.3.8 Configuration Examples for URL Filtering

### 7.3.8.1 Example for Configuring URL Filtering to Regulate Online Behaviors of Employees

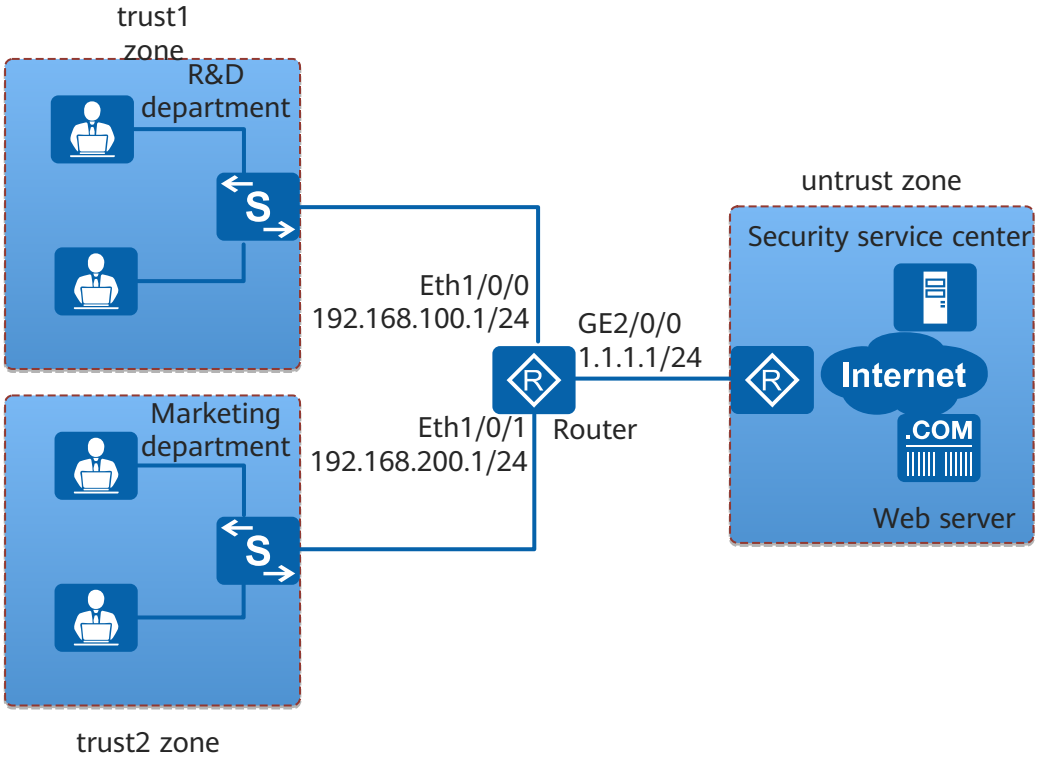
### Networking Requirements

As shown in **Figure 7-12**, the Router as the gateway is deployed at the enterprise network edge. Online behaviors of users who access web resources through HTTP need to be regulated.

The company has R&D and marketing departments. The requirements are as follows:

- All employees are allowed to access websites containing huawei.com.
- All employees are prevented from accessing websites containing youtube.com.
- R&D employees are allowed to access only www.google.com websites.
- Marketing employees are allowed to access only education/science, search/portal, and social focus websites from 09:00 to 17:00 at workdays.

**Figure 7-12** Networking for configuring URL filtering to regulate online behaviors of employees





Copyright © Huawei Technologies Co., Ltd.

## Configuration Roadmap

The configuration roadmap is as follows:

1. Divide the R&D department, marketing department, and external network in **trust1**, **trust2**, and **untrust** zones, and add interfaces to different zones so that the device monitors network traffic of the R&D department, marketing department, and external network.
2. Configure a URL filtering profile **research** for the R&D department.
   a. Add URLs containing huawei.com to the whitelist to allow employees to access these websites.
   b. Add URLs containing youtube.com to the blacklist to prevent employees from accessing these websites.
   c. Add www.google.com to customized URL category and set the action to permit.
   d. Configure URL filtering for all the websites not included in URL categories and set the action to block.
3. Configure a URL filtering profile **market** for the marketing department.
   a. Add URLs containing huawei.com to the whitelist to allow employees to access these websites.
   b. Add URLs containing youtube.com to the blacklist to prevent employees from accessing these websites.
   c. Configure URL filtering for the education/science, search/portal, and social focus websites mentioned in this example and set the action to permit.
   d. Configure URL filtering for all the websites not included in URL categories and set the action to block.
4. Configure objects requiring content security detection, that is, the time range in which content detection needs to be performed.
5. Configure two security policies **test1** and **test2**, bind them to URL filtering profiles **research** and **market** respectively, and reference the objects to perform content security detection for network traffic.
6. Apply the security policy **test1** between **trust1** and **untrust** zones and the security policy **test2** between **trust2** and **untrust** zones to control Internet access.

## Procedure

**Step 1** Upgrade the SA signature database locally. By default, the SA signature database is stored in sd1:/default-sdb/sa-sdb.zip.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] engine enable
[Router] update local sa-sdb file sd1:/default-sdb/sa-sdb.zip
```

**Step 2** Create zones.

# Create **trust1**, **trust2**, and **untrust** zones.

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router] firewall zone trust1
[Router-zone-trust1] priority 14
[Router-zone-trust1] quit
[Router] firewall zone trust2
[Router-zone-trust2] priority 10
[Router-zone-trust2] quit
[Router] firewall zone untrust
[Router-zone-untrust] priority 1
[Router-zone-untrust] quit
```

**Step 3** Assign IP addresses to interfaces and add interfaces to the zones.

# Assign IP addresses to Ethernet1/0/0, Ethernet1/0/1, and GE2/0/0, add Ethernet1/0/0 to the **trust1** zone, GE1/0/2 to the **trust2** zone, and GE2/0/0 to the **untrust** zone.

```
[Router] interface ethernet 1/0/0
[Router-Ethernet1/0/0] ip address 192.168.100.1 24
[Router-Ethernet1/0/0] zone trust1
[Router-Ethernet1/0/0] quit
[Router] interface ethernet 1/0/1
[Router-Ethernet1/0/1] ip address 192.168.200.1 24
[Router-Ethernet1/0/1] zone trust2
[Router-Ethernet1/0/1] quit
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] ip address 1.1.1.1 24
[Router-GigabitEthernet2/0/0] zone untrust
[Router-GigabitEthernet2/0/0] quit
```

**Step 4** Configure URL filtering.

# Configure a user-defined URL category named **url_userdefine_category** and add www.google.com to **url_userdefine_category**.

```
[Router] url-filter category user-defined name url_userdefine_category
[Router-category-user-defined-url_userdefine_category] add url www.google.com
[Router-category-user-defined-url_userdefine_category] quit
```

# Configure a URL filtering profile named **research** to filter traffic from R&D employees.

```
[Router] profile type url-filter name research
[Router-profile-url-filter-research] add whitelist url *huawei.com*
[Router-profile-url-filter-research] add blacklist url *youtube.com*
[Router-profile-url-filter-research] category pre-defined action block
[Router-profile-url-filter-research] category user-defined action block
[Router-profile-url-filter-research] category user-defined name url_userdefine_category action allow
[Router-profile-url-filter-research] default action block
[Router-profile-url-filter-research] quit
```

# Configure a URL filtering profile named **market** to filter traffic from marketing employees.

**NOTE**

In the **display url-filter category pre-defined** command output, the IDs of social focus, search/portal, and education/science categories are 5, 15 and 17.

When configuring the predefined URL category, run the **import url-sdb file** command in the system view to import the URL predefined URL category database to the cache of the device. By default, the URL predefined URL category database is stored in sd1:/default-sdb/url.sdb. Therefore, you need to run the **import url-sdb file sd1:/default-sdb/url.sdb** command.

```
[Router] profile type url-filter name market
[Router-profile-url-filter-market] add whitelist url *huawei.com*
[Router-profile-url-filter-market] add blacklist url *youtube.com*
[Router-profile-url-filter-market] category pre-defined action block
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router-profile-url-filter-market] category pre-defined category-id 5 action allow
[Router-profile-url-filter-market] category pre-defined category-id 15 action allow
[Router-profile-url-filter-market] category pre-defined category-id 17 action allow
[Router-profile-url-filter-market] default action block
[Router-profile-url-filter-market] quit
```

**Step 5** Configure objects requiring content security detection.

# Configure the device to perform content security detection for all traffic passing through the device from 9:00 to 17:00 at workdays.

```
[Router] time-range test 09:00 to 17:00 working-day
[Router] acl 2000
[Router-acl-basic-2000] rule 5 permit time-range test
[Router-acl-basic-2000] quit
```

**Step 6** Bind URL filtering profiles to security policies.

# Create a security policy named **test1** and bind the URL filtering profile **research** to the security policy **test1**.

```
[Router] security-policy test1
[Router-security-policy-test1] profile urlf research
[Router-security-policy-test1] quit
```

# Create a security policy named **test2** and bind the URL filtering profile **market** to the security policy **test2**.

```
[Router] security-policy test2
[Router-security-policy-test2] profile urlf market acl 2000
[Router-security-policy-test2] quit
```

**Step 7** Apply security policies to interzones.

# Apply the security policy **test1** between **trust1** and **untrust** zones.

```
[Router] firewall interzone trust1 untrust
[Router-interzone-trust1-untrust] security-policy test1
[Router-interzone-trust1-untrust] quit
```

# Apply the security policy **test2** between **trust2** and **untrust** zones.

```
[Router] firewall interzone trust2 untrust
[Router-interzone-trust2-untrust] security-policy test2
[Router-interzone-trust2-untrust] quit
```

**Step 8** Commit the configuration.

```
[Router] engine configuration commit
```

**Step 9** Verify the configuration.

- All employees can access websites containing huawei.com.
- None of employees can access websites containing youtube.com.
- R&D employees can access websites containing huawei.com and huawei.com, but cannot access other websites.
- Marketing employees can access education/science, search/portal, and social focus websites and websites containing huawei.com from 09:00 to 17:00 at workdays, but cannot access other websites.

**----End**

## Configuration Files

# Configuration file of the Router

 Copyright © Huawei Technologies Co., Ltd. 

```
#
 sysname Router
#
 time-range test 09:00 to 17:00 working-day
#
 engine enable
#
acl number 2000
 rule 5 permit time-range test
#
url-filter category user-defined name url_userdefine_category
 add url www.google.com
#
profile type url-filter name research
 add blacklist url *youtube.com*
 add whitelist url *huawei.com*
 ...
 default action block
profile type url-filter name market
 add blacklist url *youtube.com*
 add whitelist url *huawei.com*
 category pre-defined subcategory-id 101 action block
 category pre-defined subcategory-id 102 action block
 category pre-defined subcategory-id 162 action block
 ...
 default action block
#
security-policy test1
  profile urlf research
security-policy test2
  profile urlf market acl 2000
#
firewall zone trust2
 priority 10
#
firewall zone untrust
 priority 1
#
firewall zone trust1
 priority 14
#
firewall interzone trust1 untrust
 security-policy test1
#
firewall interzone trust2 untrust
 security-policy test2
#
interface Ethernet1/0/0
 ip address 192.168.100.1 255.255.255.0
 zone trust1
#
interface Ethernet1/0/1
 ip address 192.168.200.1 255.255.255.0
 zone trust2
#
interface GigabitEthernet2/0/0
 ip address 1.1.1.1 255.255.255.0
 zone untrust
#
return
```

 Copyright © Huawei Technologies Co., Ltd. 

# 8 Local Attack Defense Configuration

## About This Chapter

This chapter describes how to configure local attack defense to limit the rate of packets reaching the CPU. This function protects device security and ensures uninterrupted services.

8.1 Overview of Local Attack Defense

8.2 Licensing Requirements and Limitations for Local Attack Defense

8.3 Default Settings for Local Attack Defense

8.4 Configuring CPU Attack Defense
With the CPU attack defense function, the device limits the rate of packets sent to the CPU to protect the CPU.

8.5 Configuring Attack Source Tracing
After attack source tracing is configured on a device, the device analyzes packets sent to the CPU and sends logs or alarms to notify the administrator of the potential attack packets so that the administrator can take protective measures.

8.6 Maintaining Local Attack Defense

8.7 Configuration Examples for Local Attack Defense

8.8 Troubleshooting Local Attack Defense

8.9 FAQ About Local Attack Defense

## 8.1 Overview of Local Attack Defense

### Definition

Local attack defense protects the CPU of a device and prevents service interruption caused by attacks from a large number of packets or malicious packets.

Device CPUs need to process a large number of packets including valid packets and malicious attack packets on a network. The malicious attack packets

 Copyright © Huawei Technologies Co., Ltd. 

overwhelm the CPUs, and thus affect services and cause a system breakdown. In addition, excessive valid packets can also lead to high CPU usage, which degrades the CPU's performance and interrupts services.

To ensure that the CPU can process services in a timely manner, the device provides a local attack defense function. When a device is undergoing an attack, this function ensures uninterrupted service transmission and minimizes the impact on network services.

## Basic Implementation

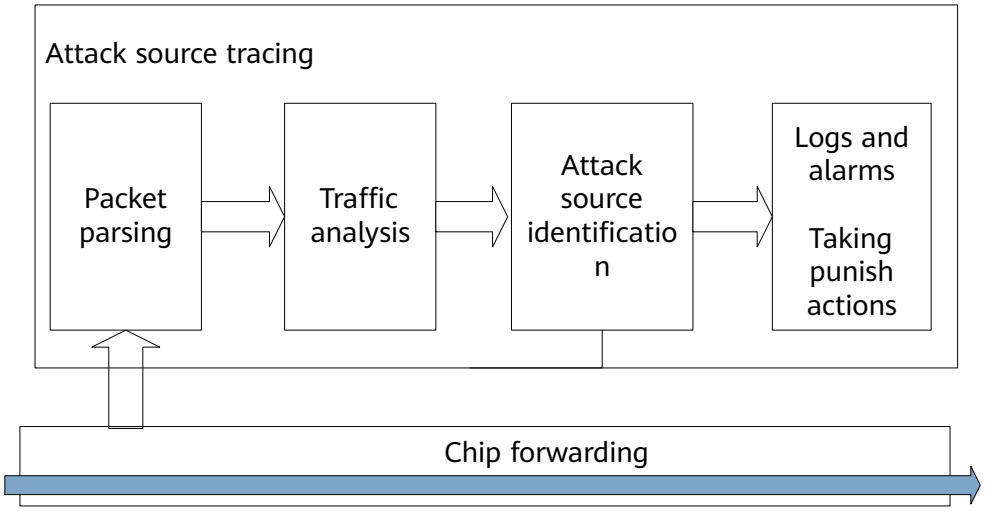
The device supports two types of local attack defense: CPU attack defense and attack source tracing.

- The device can limit the rate of all packets sent to the CPU to protect the CPU.
  a. The device provides hierarchical device protection:
     - Level 1: The device filters invalid packets sent to the CPU using blacklists.
     - Level 2: The device limits the rate of packets sent to the CPU based on the protocol type to prevent excess packets of a protocol from being sent to the CPU.
     - Level 3: The device schedules packets sent to the CPU based on priorities of protocol packets to ensure that packets with higher protocol priorities are processed first.
     - Level 4: The device uniformly limits the rate of packets with the same priority sent to the CPU and randomly discards the excess packets to protect the CPU.
  b. When the device detects setup of a Telnet, SSH. HTTP, FTP, or BGP session, ALP is enabled to protect the session. The packets matching characteristics of the session are sent at a high rate; therefore, reliability and stability of session-related services are ensured.
- The attack source tracing function protects the CPU against Denial of Service (DoS) attacks. The device enabled with attack source tracing analyzes packets sent to the CPU, collects statistics on the packets, and sets a rate threshold for the packets. The device considers excess packets as attack packets. The device finds the source user address or source interface of the attack by analyzing the attack packets and generates logs or alarms. Accordingly, the network administrator can take measures to defend against the attacks, for example, discarding packets from the attack source.

  Attack source tracing involves four processes shown in **Figure 8-1**: packet parsing, traffic analysis, attack source identification, log & alarm generation as well as taking **punish** actions.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 8-1** Attack source tracing processes




The device locates the attack source, and the network administrator limits the rate of packets sent from the attack source by configuring ACLs or blacklists to protect the CPU.

# 8.2 Licensing Requirements and Limitations for Local Attack Defense

## Involved Network Elements

Other network elements are not required.

## Licensing Requirements

Local attack defense is a basic feature of the router and is not under license control.

## Feature Limitations

None

# 8.3 Default Settings for Local Attack Defense

**Table 8-1** and **Table 8-2** list the default settings for local attack defense. The default settings can be modified as required.


Copyright © Huawei Technologies Co., Ltd.

**Table 8-1** Default settings for CPU attack defense

| Parameter | Default Setting |
| --- | --- |
| CPU attack defense policy | CPU attack defense policy named **default** |
| Blacklist | None |
| Rate limiting and protocol priority | The CPU attack defense policy limits the rates of different types of packets sent to the CPU, and the default rate and priority are the same as those in the **default** policy. To view the default rate and priority settings, run the **display cpu-defend configuration** command. |
| Rate limiting | • AR100&AR120&AR150&AR160&AR200 series: 1000pps<br>• AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204-51GE, AR2204E-D, and AR2204: 1000pps<br>• AR2220, AR2220L, and AR2220E: 1500pps<br>• AR2204XE and AR2204XE-DC: 2000pps<br>• For the AR2240 and AR3260, the rate limit for all packets sent to the CPU depending on different SRUs.<br>– SRU40 and SRU60: 1500pps<br>– SRU80 and SRU100E: 2000pps<br>– SRU200, SRU200E, and SRU400: 2500pps<br>• AR2240C: 1500pps<br>• For the AR3600: 2500pps |


Copyright © Huawei Technologies Co., Ltd.

| Parameter | Default Setting |
| --- | --- |
| Rate limits used after ALP is enabled | The default rate limit of SSH, Telnet, SSHv6, Telnetv6, HTTP, FTP, IKE, or BGP packets.<br>• SSH: 512 pps<br>• Telnet: 512 pps<br>• SSHv6: 512 pps<br>• Telnetv6: 512 pps<br>• HTTP: 512pps<br>• FTP: 1024pps<br>• IKE: 128pps<br>• BGP: 512pps<br>Modified the default rate limit used the **application-apperceive** command. |

**Table 8-2** Default configuration for attack source tracing

| Parameter | Default Setting |
| --- | --- |
| Attack defense policy | Attack defense policy named **default** |
| Automatic attack source tracing | Disabled |
| Threshold for attack source tracing | 128 pps |
| Attack source tracing mode | Attack source tracing based on source MAC addresses, source IP addresses, or a combination of source ports and VLANs |
| Types of traced packets | ARP, DHCP, ICMP, IGMP, Telnet, TCP, and TTL-expired packets |
| Alarm function for attack source tracing | Disabled |
| Alarm threshold for attack source tracing | 128 pps |
| Punish function for attack source tracing | Disabled |

# 8.4 Configuring CPU Attack Defense

With the CPU attack defense function, the device limits the rate of packets sent to the CPU to protect the CPU.


Copyright © Huawei Technologies Co., Ltd.

### Pre-configuration Tasks

Before configuring CPU attack defense, complete the following tasks:

- Connect interfaces and set physical parameters for the interfaces to ensure that the physical status of the interfaces is Up.
- Configure an ACL for blacklist, if necessary.

### Configuration Procedure

Before configuring CPU attack defense, create an attack defense policy. The other tasks can be performed in any sequence and can be selected as required. An attack defense policy takes effect only after it is applied to an object. There is no limitation on when the attack defense policy is applied.

## 8.4.1 Creating an Attack Defense Policy

### Context

Before configuring the local attack defense function, you must create an attack defense policy.

NOTE

The attack defense policy does not take effect for protocol packets sent from 3G cellular interfaces to the CPU of the MPU.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend policy** *policy-name*

An attack defense policy is created and the attack defense policy view is displayed.

The device supports a maximum of 19 attack defense policies, including the **default** attack defense policy. By default, the **default** attack defense policy is applied to all boards and cannot be deleted or modified. The other 18 policies can be modified or deleted.

**Step 3** (Optional) Run **description** *text*

The description of the attack defense policy is configured.

By default, an attack defense policy does not have a description.

**----End**

## 8.4.2 Configuring a Blacklist

### Context

A blacklist is a group of users with particular characteristics. The device discards packets from users in the blacklist. You can apply an ACL to a blacklist.

 Copyright © Huawei Technologies Co., Ltd. 

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend policy** *policy-name*

The attack defense policy view is displayed.

**Step 3** Run **blacklist** *blacklist-id* **acl** *acl-number*

A blacklist is created.

A maximum of eight blacklists can be configured on the device.

The ACL applied to a blacklist can be a basic ACL, an advanced ACL, or a Layer 2 ACL. For details on how to create an ACL, see **5 ACL Configuration**.

By default, no blacklist is configured on the device.

**----End**

## 8.4.3 Configuring Dynamic CPCAR Adjustment

### Context

When CPCAR values are manually set, a device cannot immediately control the rate of packets sent to the CPU when undergoing an attack. As a result, the CPU usage exceeds the acceptable range and CPU performance degrades.

After dynamic CPCAR adjustment is configured, the device periodically checks CPU usage, and automatically adjusts CPCAR values of protocol packets when the CPU usage exceeds the specified upper threshold, reducing impact on the CPU.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend policy** *policy-name*

The attack defense policy view is displayed.

**Step 3** Run **rate-adaption enable**

Dynamic CPCAR adjustment is enabled.

By default, dynamic CPCAR adjustment is disabled.

**Step 4** Run **rate-adaption adjust-period** *period-value*

The interval for checking CPU usage is set.

By default, the interval for checking CPU usage is 30 seconds.

**Step 5** Run **rate-adaption cpu-usage threshold low** *low-value* **high** *high-value*

 Copyright © Huawei Technologies Co., Ltd. 

The CPU usage thresholds are set. When the CPU usage exceeds the upper threshold or falls below the lower threshold, the device automatically adjusts the CPCAR values.

By default, the lower threshold is 65% and the upper threshold is 85%.

**Step 6** Run **rate-adaption adjust-step** *step-value*

The dynamic CPCAR adjustment step is set.

By default, the dynamic CPCAR adjustment step is 20%.

**Step 7** (Optional) Run **rate-adaption exception packet-type** *packet-type*

The protocols excluded from dynamic CPCAR adjustment are specified. The CPCAR values for these protocols are not dynamically adjusted.

By default, the CPCAR values for all protocol packets are dynamically adjusted.

**----End**

## 8.4.4 Configuring the Rate Limit for Packets Sent to the CPU

### Context

The device applies different rate limits to packets of different types or discards packets of a specified type to protect the CPU.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend policy** *policy-name*

The attack defense policy view is displayed.

**Step 3** Configure a rate limit for packets sent to the CPU.

- Run **packet-type** *packet-type* **rate-limit** *rate-value*

  The rate limit for packets sent to the CPU is set. Excess packets are discarded.
- Run **deny packet-type** *packet-type*

  The device is configured to discard packets of a specified type sent to the CPU. That is, the rate limit for packets sent to the CPU is 0.

By default, the device applies the rate limit defined in the **default** attack defense policy to limit the packets sent to the CPU.

**----End**

## 8.4.5 Setting the Priority for Packets of a Specified Protocol

### Context

After an attack defense policy is created, set priorities of protocol packets in the attack defense policy so that packets with higher priorities are processed first.

 Copyright © Huawei Technologies Co., Ltd. 

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend policy** *policy-name*

The attack defense policy view is displayed.

**Step 3** Run **packet-type** *packet-type* **priority** *priority-level*

The priority for packets of a specified protocol sent to the CPU is set.

By default, the priority defined in the **default** attack defense policy is used for packets of a specified protocol sent to the CPU.

**----End**

## 8.4.6 Configuring ALP

### Context

Active link protection (ALP) protects session-based application layer data, including data of SSH sessions, Telnet sessions, SSHv6 sessions, Telnetv6 sessions, HTTP sessions, IKE sessions, BGP sessions, and FTP sessions to ensure uninterrupted services when attacks occur.

The rate limit for packets after ALP is enabled can be set in the attack defense policy view and applied to the LPU or MPU with attack defense policy. The **cpu-defend application-apperceive** command enables the ALP function.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend policy** *policy-name*

The attack defense policy view is displayed.

**Step 3** (Optional) Run **cpu-defend application-apperceive** [ **ssh** | **telnet** | **sshv6** | **telnetv6** | **bgp** | **ftp** | **http** | **ike** ] **enable**

ALP is enabled.

By default, ALP is enabled for SSH, Telnet, SSHv6, Telnetv6, FTP, BGP, IKE, and HTTP.

NOTE

V200R010C10 and later versions support the **ike** parameter.

**Step 4** Run **application-apperceive packet-type** { **ssh** | **telnet** | **sshv6** | **telnetv6** | **bgp** | **ftp** | **http** | **ike** } **rate-limit** *rate-value*

The rate limit for SSH packets, Telnet packets, SSHv6 packets, Telnetv6 packets, HTTP packets, BGP packets, IKE packets, or FTP packets is set.

 Copyright © Huawei Technologies Co., Ltd. 

By default, the rate limit for SSH packets, Telnet packets, SSHv6 packets, Telnetv6 packets, HTTP packets, BGP packets is 512 pps, the rate limit for IKE packets is 128 pps, and the rate limit for FTP packets is 1024 pps.

NOTE

If this command is not configured, the default rate limit specified by **application-apperceive** is applied to SSH, Telnet, SSHv6, Telnetv6, HTTP, FTP, IKE, or BGP packets.

After ALP is configured for FTP packets, it also takes effect for TFTP packets.

V200R010C10 and later versions support the **ike** parameter.

**----End**

# 8.4.7 Configuring the Rate Limit for All Packets Sent to the CPU

## Context

After an attack defense policy is created, set the rate limit for all packets sent to the CPU in the attack defense policy. The device uniformly limits the rate of packets with the same priority sent to the CPU and randomly discards the excess packets to protect the CPU.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend policy** *policy-name*

The attack defense policy view is displayed.

**Step 3** Run **rate-limit all-packets pps** *pps-value*

The rate limit for all packets sent to the CPU is set.

By default, the rate limit for all packets sent to the CPU is as follows:

- AR100&AR120&AR150&AR160&AR200 series: 1000pps
- AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, and AR2204: 1000pps
- AR2220, AR2240C: 1500pps
- AR2204XE, and AR2204XE-DC: 2000pps
- For the AR2240 and AR3260, the rate limit for all packets sent to the CPU depending on different SRUs.
  - SRU40: 1500pps
  - SRU80 and SRU100E: 2000pps
  - SRU200, SRU200E, and SRU400: 2500pps
- AR3600: 2500pps

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## 8.4.8 Applying an Attack Defense Policy

### Context

After an attack defense policy is created, you must apply the attack defense policy to the SRU or all LAN-side interface cards in the system view, or specified LAN-side interface cards. Otherwise, the attack defense policy does not take effect.

NOTE

- If the attack defense policy is applied to a LAN-side interface card or SRU, the policy takes effect for only the packets sent to the CPU of the LAN-side interface card or SRU.
- If the LAN-side interface card and SRU both support attack defense policy, you are advised to apply an attack defense policy to both of them.
- If the attack defense policy is applied to a LAN-side interface card or SRU, the policy takes effect for only the packets sent to the CPU of the LAN-side interface card or SRU.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend-policy** *policy-name* [ **global** | **slot** *slot-id* ]

The attack defense policy is applied.

**----End**

## 8.4.9 Verifying the CPU Attack Defense Configuration

### Procedure

- Run the **display cpu-defend policy** [ *policy-name* ] command to check the attack defense policy.
- Run the **display cpu-defend statistics** [ **packet-type** *packet-type* ] command to check statistics on packets sent to the CPU.
- Run the **display cpu-defend configuration** [ **packet-type** *packet-type* ] { **all** | **slot** *slot-id* | **sru** } command to check the rate limits for protocol packets sent to the CPU.
- Run the **display cpu-defend rate-adaption statistics** [ **packet-type** *packet-type* ] command to check statistics on packet rate after CPCAR settings are dynamically adjusted.

**----End**

# 8.5 Configuring Attack Source Tracing

After attack source tracing is configured on a device, the device analyzes packets sent to the CPU and sends logs or alarms to notify the administrator of the potential attack packets so that the administrator can take protective measures.

 Copyright © Huawei Technologies Co., Ltd. 

### Pre-configuration Tasks

Before configuring attack source tracing, connect interfaces and set physical parameters for the interfaces to ensure that the physical status of the interfaces is Up.

### Configuration Procedure

To configure attack source tracing, you must create an attack defense policy. All other configuration tasks are optional and are not listed in sequence. An attack defense policy takes effect only after it is applied to an object. There is no limitation on when the attack defense policy is applied.

## 8.5.1 Creating an Attack Defense Policy

### Context

Before configuring the local attack defense function, you must create an attack defense policy.

NOTE

The attack defense policy does not take effect for protocol packets sent from 3G cellular interfaces to the CPU of the MPU.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend policy** *policy-name*

An attack defense policy is created and the attack defense policy view is displayed.

The device supports a maximum of 19 attack defense policies, including the **default** attack defense policy. By default, the **default** attack defense policy is applied to all boards and cannot be deleted or modified. The other 18 policies can be modified or deleted.

**Step 3** (Optional) Run **description** *text*

The description of the attack defense policy is configured.

By default, an attack defense policy does not have a description.

**----End**

## 8.5.2 Configuring the Threshold for Attack Source Tracing

### Context

Attackers may send a large number of packets to attack network devices' CPUs. You can configure attack source tracing and set an alarm threshold for attack source tracing so that the device can analyze packets sent to the CPU. If the number of protocol packets sent from an attack source in a specified period

 Copyright © Huawei Technologies Co., Ltd. 

exceeds the alarm threshold, the device sends logs or alarms to notify the administrator so that the administrator can take measures to prevent attacks.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend policy** *policy-name*

The attack defense policy view is displayed.

**Step 3** Run **auto-defend enable**

Attack source tracing is enabled.

By default, attack source tracing is disabled.

**Step 4** Run **auto-defend threshold** *threshold*

The checking threshold for attack source tracing is set.

By default, the checking threshold for attack source tracing is 128 pps.

**----End**

## 8.5.3 Configuring an Attack Source Tracing Mode

### Context

After attack source tracing is enabled, you need to set a mode in which the device traces attack sources. The device supports the following attack source tracing modes:

- Source IP address-based tracing: prevents Layer 3 attack packets.
- Source MAC address-based tracing: prevents Layer 2 attack packets with a fixed source MAC address.
- Tracing based on a combination of source port and VLAN: prevents Layer 2 attack packets with different source MAC addresses.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend policy** *policy-name*

The attack defense policy view is displayed.

**Step 3** Run **auto-defend enable**

Attack source tracing is enabled.

By default, attack source tracing is disabled.

**Step 4** Run **auto-defend trace-type** { **source-ip** | **source-mac** | **source-portvlan** } *

The attack source tracing mode is specified.

By default, the device traces attack sources based on source MAC addresses, source IP addresses, and a combination of source ports+VLANs.

NOTE

By default, all the three attack source tracing modes take effect. If only one attack source tracing mode is needed, run the **undo auto-defend trace-type** command to delete the unnecessary attack source tracing modes. If the unnecessary modes are not deleted, the involved interface will be set to Down and services on the interface will become unavailable.

**----End**

# 8.5.4 Configuring the Types of Traced Packets

## Context

When an attack occurs, the device traces packets of all types, and the administrator cannot identify the type of attack packets. You can specify the types of packets that the device traces.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend policy** *policy-name*

The attack defense policy view is displayed.

**Step 3** Run **auto-defend enable**

Attack source tracing is enabled.

By default, attack source tracing is disabled.

**Step 4** Run **auto-defend protocol** { **all** | { **arp** | **dhcp** | **icmp** | **igmp** | **ospf** | **tcp** | **telnet** | **ttl-expired** } * }

The type of traced packets is specified.

By default, the device traces sources of ARP, DHCP, ICMP, IGMP, OSPF, TCP, Telnet, and TTL-expired packets in attack source tracing.

**----End**

# 8.5.5 Configuring Event Reporting Function

## Context

This function sends an event report to the administrator when the rate of packets of a specified protocol sent by an attack source exceeds the configured threshold, so that the administrator can take measures in time to protect the device.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend policy** *policy-name*

The attack defense policy view is displayed.

**Step 3** Run **auto-defend enable**

Attack source tracing is enabled.

By default, attack source tracing is disabled.

**Step 4** Configure the event reporting function for attack source tracing.

1. Run **auto-defend alarm enable**

   The event reporting function for attack source tracing is enabled.

   By default, the event reporting function for attack source tracing is disabled.
2. Run **auto-defend alarm threshold** *threshold*

   The event reporting threshold for attack source tracing is set.

   By default, the event reporting threshold for attack source tracing is 128 pps.

**----End**

# 8.5.6 Configuring Attack Source Punish Actions

## Context

After you configure **punish** actions on a device, the device discards packets sent from the attacker to prevent attacks.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend policy** *policy-name*

The attack defense policy view is displayed.

**Step 3** Run **auto-defend enable**

Attack source tracing is enabled.

By default, attack source tracing is disabled.

**Step 4** Run **auto-defend action deny** [ **timer** *time-length* ]

The **punish** function is enabled.

By default, the **punish** function is disabled.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## 8.5.7 Applying an Attack Defense Policy

### Context

After an attack defense policy is created, you must apply the attack defense policy to the SRU or all LAN-side interface cards in the system view, or specified LAN-side interface cards. Otherwise, the attack defense policy does not take effect.

NOTE

If the attack defense policy is applied to a LAN-side interface card or SRU, the policy takes effect for only the packets sent to the CPU of the LAN-side interface card or SRU.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **cpu-defend-policy** *policy-name* [ **global** | **slot** *slot-id* ]

The attack defense policy is applied.

**----End**

## 8.5.8 Verifying the Attack Source Tracing Configuration

### Procedure

- Run the **display auto-defend attack-source** [ **detail** ] command to check attack sources on the SRU.
- Run the **display auto-defend configuration** [ **cpu-defend policy** *policy-name* ] command to check the configuration of attack source tracing in an attack defense policy.
- Run the **display cpu-defend policy** [ *policy-name* ] command to check the attack defense policy.

**----End**

# 8.6 Maintaining Local Attack Defense

## 8.6.1 Clearing Attack Source Information

### Context

Before collecting updated statistics on attack sources, run the following command in the user view to clear the existing statistics.

 Copyright © Huawei Technologies Co., Ltd. 

NOTICE

The cleared attack source information cannot be restored. Exercise caution when you use the command.

### Procedure

**Step 1** Run the **reset auto-defend attack-source** command to clear information about the attack sources on the main control board.

**----End**

## 8.6.2 Clearing Statistics About Packets Sent to the CPU

### Context

Before collecting updated statistics on packets sent to the CPU, run the following command in the user view to clear the existing statistics.

NOTICE

The cleared statistics cannot be restored. Exercise caution when you use the command.

### Procedure

**Step 1** Run the **reset cpu-defend statistics** [ **packet-type** *packet-type* ] command to clear statistics about packets sent to the CPU.

**----End**

# 8.7 Configuration Examples for Local Attack Defense

## 8.7.1 Example for Configuring Local Attack Defense

### Networking Requirements

As shown in **Figure 8-2**, users on different LANs access the Internet through RouterA. To locate attacks on RouterA, attack source tracing needs to be configured to trace the attack source. The following situations occur:

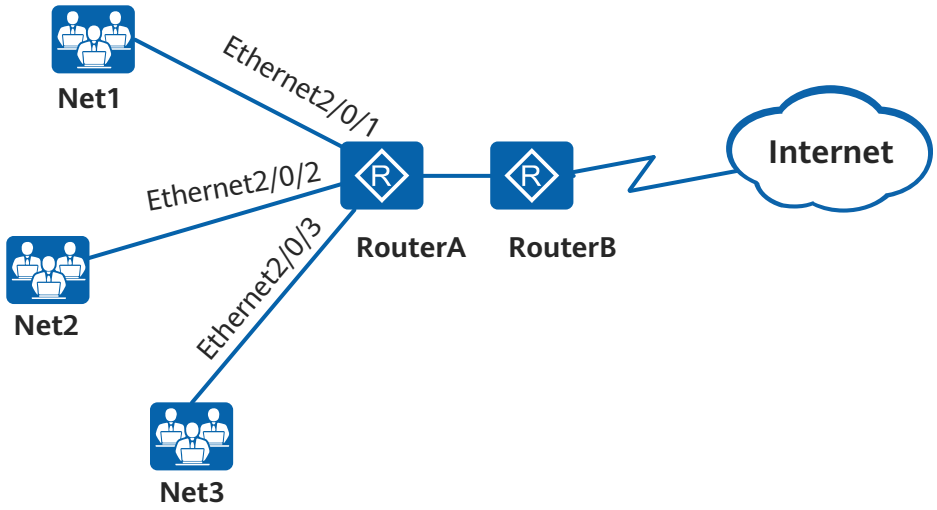
- A user on Net1 frequently initiates attacks to RouterA.
- The attacker sends a large number of ARP Request packets, degrading CPU performance.
- The administrator needs to upload files to RouterA using FTP. An FTP connection between the administrator's host and RouterA needs to be set up.

 Copyright © Huawei Technologies Co., Ltd. 

- Most LAN users obtain IP addresses using DHCP, whereas RouterA does not first process dhcp-client packets sent to the CPU.
- The Telnet server is not enabled on the RouterA, whereas RouterA often receives a large number of Telnet packets.

Configurations need to be performed on RouterA to solve the preceding problems.

**Figure 8-2** Networking diagram for configuring local attack defense




## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a blacklist and add attackers on Net1 to the blacklist to prevent users on Net1 from accessing the network.
2. Configure the rate limit for ARP Request packets sent to the CPU to ensure that the CPU can process normal services.
3. Configure active link protection (ALP) for FTP so that file data can be transmitted between the administrator's host and RouterA.
4. Configure a high priority for dhcp-client packets so that RouterA first processes dhcp-client packets sent to the CPU.
5. Disable the Telnet server on the RouterA so that RouterA discards all received Telnet packets.

## Procedure

**Step 1** Configure an ACL to be referenced by the blacklist.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] acl number 4001
[RouterA-acl-L2-4001] rule 5 permit source-mac 0001-c0a8-0102
[RouterA-acl-L2-4001] quit
```

**Step 2** Create an attack defense policy.

```
[RouterA] cpu-defend policy devicesafety
```

 Copyright © Huawei Technologies Co., Ltd. 

**Step 3** Configure the alarm threshold for attack source tracing.

```
[RouterA-cpu-defend-policy-devicesafety] auto-defend enable
[RouterA-cpu-defend-policy-devicesafety] auto-defend threshold 50
```

**Step 4** Configure a blacklist.

```
[RouterA-cpu-defend-policy-devicesafety] blacklist 1 acl 4001
```

**Step 5** Configure the rate limit for ARP Request packets sent to the CPU.

```
[RouterA-cpu-defend-policy-devicesafety] packet-type arp-request rate-limit 64
```

**Step 6** Configure the rate limit for FTP packets after ALP is enabled.

```
[RouterA-cpu-defend-policy-devicesafety] application-apperceive packet-type ftp rate-limit 2000
```

**Step 7** (Optional) Set the attack source tracing mode.

```
[RouterA-cpu-defend-policy-devicesafety] auto-defend trace-type source-mac
[RouterA-cpu-defend-policy-devicesafety] undo auto-defend trace-type source-ip source-portvlan
```

NOTE

By default, all the three attack source tracing modes take effect. If only one attack source tracing mode is needed, run the **undo auto-defend trace-type** command to delete the unnecessary attack source tracing modes. If the unnecessary modes are not deleted, the involved interface will be set to Down and services on the interface will become unavailable.

**Step 8** Set the priority of dhcp-client packets.

```
[RouterA-cpu-defend-policy-devicesafety] packet-type dhcp-client priority 3
[RouterA-cpu-defend-policy-devicesafety] quit
```

**Step 9** Apply the attack defense policy.

# Enable ALP for FTP.

```
[RouterA] cpu-defend application-apperceive ftp enable
```

# Apply the attack defense policy to the main control board.

```
[RouterA] cpu-defend-policy devicesafety
```

**Step 10** Disable the Telnet server.

```
[RouterA] undo telnet server enable
```

NOTE

You do not need to disable application layer association. The Router discards all received Telnet packets after the Telnet server is disabled on the Router.

**Step 11** Verify the configuration.

# View information about the configured attack defense policy.

```
[RouterA] display cpu-defend policy devicesafety
 Related slot : <0>
 BlackList Status :
   Slot<0> : Success
 Configuration :
   Blacklist 1 ACL number : 4001
   Packet-type arp-request rate-limit : 64(pps)
   Packet-type dhcp-client priority : 3
   Rate-limit all-packets : 2000(pps)(default)
   Application-apperceive packet-type ftp : 2000(pps)
   Application-apperceive packet-type tftp : 2000(pps)
```

# View the rate limit configuration on the main control board. You can see that application layer association for Telnet is configured successfully and the rate limit

 Copyright © Huawei Technologies Co., Ltd. 

for ARP Request packets sent to the CPU and the priority for dhcp-client packets are set successfully.

```
<Huawei> display cpu-defend configuration sru
Rate configurations on main board.
------------------------------------------------------------------
Packet-type             Status       Rate-limit(PPS)  Priority
------------------------------------------------------------------
8021X                   Disabled     160              2
arp-miss                Enabled      64               2
arp-reply               Enabled      128              2
arp-request             Enabled      64               2
bfd                     Disabled     512              4
bgp                     Enabled      256              3
bgp4plus                Enabled      256              3
capwap                  Enabled      512              1
dhcp-client             Enabled      128              3
......
telnet-server           Disabled     128              4
ttl-expired             Enabled      256              1
udp-helper              Disabled     32               2
unknown-multicast       Enabled      128              1
unknown-packet          Enabled      256              1
voice                   Enabled      256              4
vrrp                    Disabled     256              3
wapi                    Enabled      1024             2
x25                     Enabled      4096             1
------------------------------------------------------------------
```

# The log about attack source tracing of Net1 indicates that attack source tracing has taken effect.

```
Dec 18 2010 09:55:50-05:13 device %%01SECE/4/USER_ATTACK(l)[0]:User attack
occurred.(Slot=MPU, SourceAttackInterface=Ethernet2/0/1, OuterVlan/
InnerVlan=0/0, UserMacAddress=0001-c0a8-0102, AttackPackets=48 packets per
second)
```

# View the statistics on packets sent to the SRU. The discarded packets indicate that the rate limit is set for ARP Request packets.

```
<Huawei> display cpu-defend statistics
------------------------------------------------------------------------
Packet Type             Pass Packets       Drop Packets
------------------------------------------------------------------------
8021X                   0                  0
arp-miss                5                  0
arp-reply               8090               0
arp-request             1446576            127773
bfd                     0                  0
bgp                     0                  0
bgp4plus                0                  0
dhcp-client             879                0
dhcp-server             0                  0
dhcpv6-reply            0                  0
dhcpv6-request          0                  0
dns                     4                  0
fib-hit                 0                  0
fr                      0                  0
ftp-client              0                  0
ftp-server              0                  0
......
udp-helper              0                  0
unknown-multicast       0                  0
unknown-packet          66146              0
voice                   0                  0
vrrp                    0                  0
------------------------------------------------------------------------
```

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

### Configuration Files

Configuration files on RouterA

```
#
sysname RouterA
#
acl number 4001
 rule 5 permit source-mac 0001-c0a8-0102
#
cpu-defend policy devicesafety
 blacklist 1 acl 4001
 packet-type arp-request rate-limit 64
 packet-type dhcp-client priority 3
 application-apperceive packet-type ftp rate-limit 2000
 auto-defend enable
 auto-defend threshold 50
#
 cpu-defend-policy devicesafety
#
return
```

# 8.8 Troubleshooting Local Attack Defense

## 8.8.1 Attack Source Tracing Does Not Take Effect

### Fault Description

Attack source tracing does not take effect after attack source tracing is configured.

### Common Causes

Possible causes are as follows:

- The attack defense policy is not applied to the correct SRU.
- The checking threshold for attack source tracing is large.

### Procedure

**Step 1** Determine the attacked target.

1. Run the **display cpu-usage** command to check CPU usage of the SRU to check whether the SRU has been attacked.
2. If the SRU has been attacked, go to the next step.

**Step 2** Determine whether the attack defense policy configured with attack source tracing is applied to the attacked LPU or main control board.

1. Run the **display this** command in the system view to check whether the **cpu-defend-policy** command has been configured.
2. Or run the **display auto-defend configuration** command to check the name of the attack defense policy and the slot ID to which the policy is applied.
3. If the policy is not configured, run the **cpu-defend-policy** command in the system view to configure the policy. If the policy is configured, go to the next step.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 3** Check whether the checking threshold for attack source tracing is large.

Run the **display auto-defend configuration** command to check the value in the **auto-defend threshold** field. If the value is large, run the **auto-defend threshold** command in the attack defense policy view to reduce the value.

**----End**

## 8.8.2 The Blacklist Does Not Take Effect

### Fault Description

The configured blacklist does not take effect.

### Common Causes

Possible causes are as follows:

- Packets do not match the rules in the blacklist.
- ACL resources are insufficient.

### Procedure

**Step 1** Run the **display cpu-defend policy** *policy-name* command to check the attack defense policy.

**Step 2** Check the ACL of the blacklist in the displayed attack defense policy information, and run the **display acl** *acl-number* command to check whether service packets match the ACL rule.

**Step 3** If service packets do not match the ACL rule, run the **rule** command in the ACL view to modify the ACL rule. If service packets match the ACL rule, the blacklist may fail to be applied because ACL resources are insufficient.

**----End**

# 8.9 FAQ About Local Attack Defense

## 8.9.1 What Can I Do with Excess ACL Rules Used by a Blacklist in Local Attack Defense?

Excess ACL rules used by a blacklist do not take effect.

## 8.9.2 How Do I Configure CPCAR?

Perform the following operations to configure Control Plane Committed Access Rate (CPCAR):

- Run the **cpu-defend policy** *policy-name* command to create an attack defense policy.
- Run the **packet-type** *packet-type* **rate-limit** *rate-value* command to set the rate limit for packets sent to the CPU.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **cpu-defend-policy** *policy-name* [ **global** | **slot** *slot-id* ] command to apply the attack defense policy.

## 8.9.3 Why Does the CPCAR Rate Limit Configuration Not Take Effect?

The CPU committed access rate (CPCAR) is configured in the attack defense policy view. The CPCAR takes effect only when the attack defense policy is applied on the main control board or interface board on the local area network (LAN) side.

 Copyright © Huawei Technologies Co., Ltd. 

# 9 Attack Defense Configuration

## About This Chapter

This chapter describes how to configure attack defense to protect networks. Attack defense allows a device to identify various types of network attacks and protect itself and the connected network against malicious attacks to ensure device and network operation.

9.1 Overview of Attack Defense

9.2 Understanding Attack Defense

9.3 Application Scenarios for Attack Defense

9.4 Licensing Requirements and Limitations for Attack Defense

9.5 Default Settings for Attack Defense

9.6 Configuring Defense Against Malformed Packet Attacks

9.7 Configuring Defense Against Packet Fragment Attacks

9.8 Configuring Defense Against Flood Attacks

9.9 Clearing Attack Defense Statistics

9.10 Configuration Examples for Attack Defense

## 9.1 Overview of Attack Defense

### Definition

Attack defense is a network security feature that enables a device to analyze the content and behavior of packets sent to the CPU, identify attack packets, and take measures to block attack packets.

Attack defense prevents malformed packet attacks, packet fragment attacks, and flood attacks.

 Copyright © Huawei Technologies Co., Ltd. 

### Purpose

Attacks initiated by utilizing inherent bugs of communication protocols or improper network deployment have great impact on networks. In particular, attacks on a network device can cause the device or network to crash.

The attack defense feature discards or limits the rate of various attack packets sent to the CPU, protecting the device and ensuring normal services.

# 9.2 Understanding Attack Defense

## 9.2.1 Defense Against Malformed Packet Attacks

A malformed packet attack occurs when malformed IP packets are sent to a target system, causing the system to work abnormally or break down. With the capability of defending against such attacks, a device can detect and discard malformed packets in real time.

Malformed packet attacks are classified into the following types.

### Flood Attacks from IP Null Payload Packets

An IP null payload packet has only a 20-byte IP header, but does not have a data field. When a target system is processing such an IP packet, the system may work abnormally or crash.

After defense against malformed packet attacks is enabled, a device directly discards such packets.

### Attacks from IGMP Null Payload Packets

An IGMP packet consists of a 20-byte IP header and an 8-byte IGMP body. An IGMP null payload packet consists of less than 28 bytes. When a network device processes IGMP null payload packets, errors may occur or the device may break down.

After defense against malformed packet attacks is enabled, the device directly discards the received IGMP null payload packets.

### LAND Attacks

By utilizing the defects in the three-way handshake mechanism of TCP, a Local Area Network Denial (LAND) attacker sends an SYN packet in which the source and destination addresses are the same as the target host's address and the source port is the same as the destination port. After receiving the SYN packet, the target host creates a null TCP connection by using its own address as both the source and destination addresses. The connection is kept until expiration. The target host will create many null TCP connections after receiving a large number of such SYN packets, leading to a waste of network resources or even system breakdown.

After defense against malformed packet attacks is enabled, the device checks source and destination addresses in TCP SYN packets. The device considers TCP

 Copyright © Huawei Technologies Co., Ltd. 

SYN packets with the same source and destination addresses as malformed packets and discards them.

### Smurf Attack

An attacker sends an ICMP Request packet of which the source address is the target host's address and the destination address is the broadcast address of the target network. After all hosts on the target network receive the ICMP Request packet, they send ICMP Reply packets to the target host. The target host receives an excessive number of packets, which consume many resources, leading to a system or network breakdown.

After defense against malformed packet attacks is enabled, the device checks whether the destination addresses in ICMP Request packets are the broadcast or subnet broadcast addresses. When detecting that the destination addresses of ICMP Request packets are the broadcast addresses or subnet broadcast addresses, the device discards them.

### Attacks from Packets with Invalid TCP Flag Bits

A TCP packet contains six flag bits: URG, ACK, PSH, RST, SYN, and FIN. Different systems respond differently to the combination of these flag bits.

- If the six flag bits are all 1s, the attack is a Christmas tree attack. A device undergoing a Christmas tree attack may break down.
- An attacker sends a TCP packet in which the SYN and FIN are 1 to a target host. If the receiving port is disabled, the receiver replies with an RST | ACK message. If the receiving interface is enabled, the receiver replies with an SYN | ACK message. This attack is used to detect whether a host is online or offline and whether an interface is enabled or disabled.
- An attacker sends a TCP packet in which the six flag bits are all 0s. If the receiving interface is disabled, the receiver replies with an RST | ACK message to detect whether the host is online or offline. If the receiving interface is enabled, Linux and UNIX operating systems do not respond but the Windows operating system replies with an RST | ACK message. This attack is used to detect the type of operating system (Windows, Linux, or UNIX) on the target host.

After defense against malformed packet attacks is enabled, the device checks each flag bit in TCP packets to prevent attacks from packets with invalid TCP flag bits. If any of the following conditions is met, the device discards the TCP packets:

- The six flag bits are all 1s.
- The SYN and FIN bits are all 1s.
- The six flag bits are all 0s.

## 9.2.2 Defense Against Packet Fragment Attacks

If an attacker sends error packet fragments to a network device, the device may consume a large number of CPU resources, restart, or even break down. Defense against packet fragment attacks allows the device to detect packet fragments in real time and discard them or limit the rate of the packets to protect the device.

Attacks of packet fragments are classified into the following types.

 Copyright © Huawei Technologies Co., Ltd. 

## Excess-Fragment Attacks

The offset of IP packets is calculated on the basis of 8 bytes. Normally, an IP header has 20 bytes and the maximum payload of an IP packet is 65515 bytes. An IP packet can be fragmented into up to 8189 fragments. The device will consume many CPU resources to reassemble packets with over 8189 fragments.

After defense against packet fragment attacks is enabled, the device considers a packet with over 8189 fragments malicious and discards all fragments of the packet.

## Excess-Offset Attacks

An attacker sends a fragment with a large offset value to a target host. Then, the target host allocates memory space to store all fragments, consuming a large number of resources.

The maximum value of the offset is 65528. Generally, the offset value does not exceed 8190. If the offset value is 8189 multiplied by 8 and the IP header is 20, the last fragment can have only a 3-byte IP payload. In normal situations, the maximum value of the offset is 8189. The device considers packets with an offset value larger than 8190 malicious and discards them.

After defense against packet fragment attacks is enabled, the device checks whether the offset value multiplied by 8 is greater than 65528. If the offset value multiplied by 8 is greater than 65528, the device considers the fragments malicious and discards them.

## Repeated Packet Fragment Attacks

An attacker sends repeated fragments to a target host multiple times. There are two situations:

- The attacker sends the same fragments to a target host multiple times, causing a high CPU usage or memory error on the target host.
- The attacker sends different fragments with the same offset to a target host. The target host cannot determine which fragment is reserved, which fragment is to be discarded, and whether all fragments need to be discarded. As a result, a high CPU usage or memory error may occur on the target host.

After defense against packet fragment attacks is enabled, the device applies the committed access rate (CAR) limit to packet fragments, reserves the first fragment, and discards all the remaining repeated fragments to protect the CPU.

## Tear Drop Attack

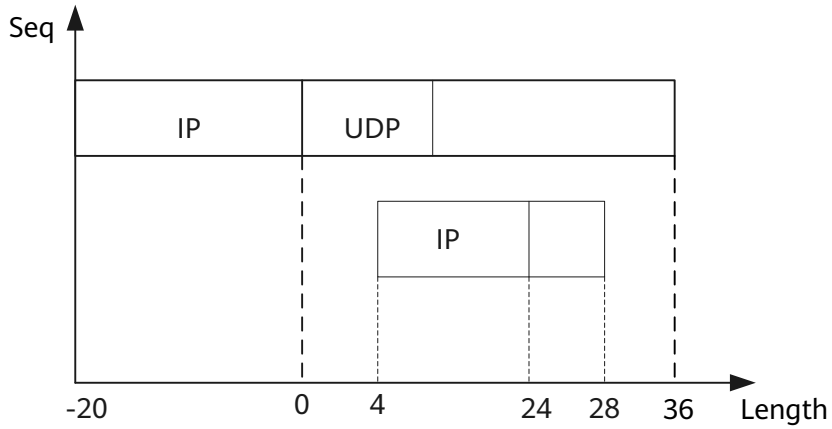
The Tear Drop attack is the frequently used IP packet fragment attack. IP packets are incorrectly fragmented and the second fragment is contained in the first one. The offset of the second fragment is smaller than that of the first fragment, and the offset plus the Data field of the second fragment does not exceed the tail of the first fragment.

As shown in **Figure 9-1**:

 Copyright © Huawei Technologies Co., Ltd. 

- The IP payload in the first fragment is 36 bytes, the total length of the IP packet is 56 bytes, the protocol is UDP, and the UDP checksum is 0 (that is, unchecked).
- The IP payload in the second fragment is 4 bytes, the total length of the IP packet is 24 bytes, the protocol is UDP, and the offset is 24 (this is incorrectly calculated and the correct offset should be 36).

**Figure 9-1** Tear Drop attack




Tear Drop attacks cause system breakdown or restart. After defense against packet fragment attacks is enabled, the device discards all the fragments in a Tear Drop attack.

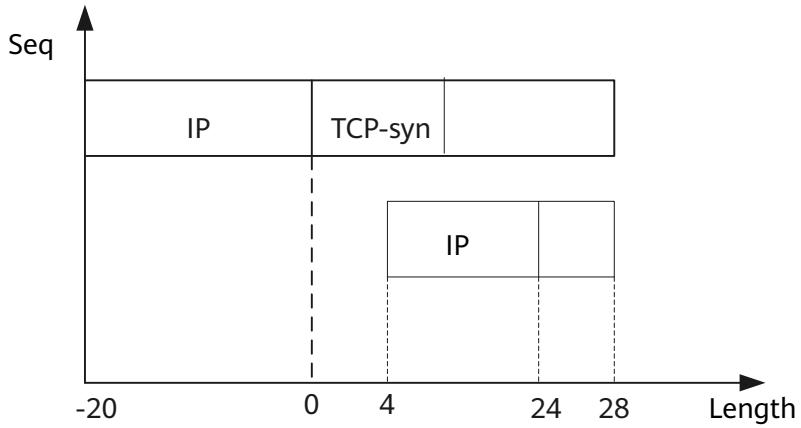
## Syndrop Attack

A Syndrop attack is similar to a Tear Drop attack except that Syndrop attacks use TCP packets with a SYN flag and IP payload.

As shown in **Figure 9-2**:

- The IP payload in the first fragment is 28 bytes, and the IP header is 20 bytes.
- The IP payload in the second fragment is 4 bytes, the IP header is 20 bytes, and the offset is 24 (this is incorrectly calculated and the correct offset should be 28).

**Figure 9-2** Syndrop attack




 Copyright © Huawei Technologies Co., Ltd. 

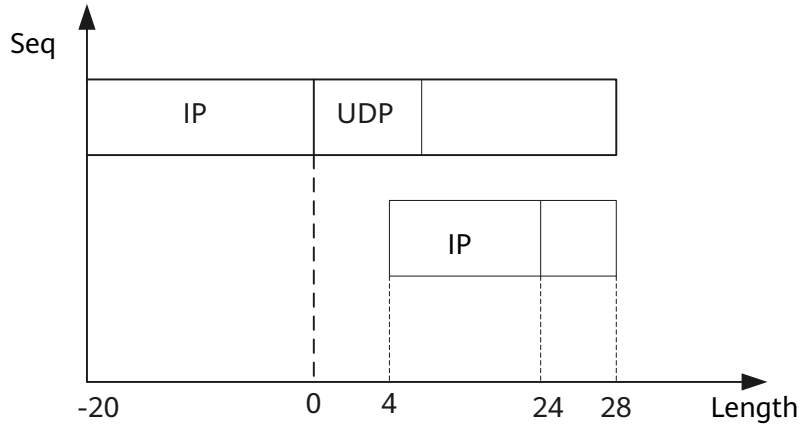
Syndrop attacks cause system breakdown or restart. After defense against packet fragment attacks is enabled, the device discards all fragments of Syndrop attacks.

## NewTear Attack

A NewTear attack uses error fragments. As shown in **Figure 9-3**, the protocol used is UDP.

- The IP payload of the first fragment is 28 bytes including the UDP header. The UDP checksum is 0.
- The IP payload of the second fragment is 4 bytes. The offset is 24, which is incorrectly calculated. The correct offset should be 28.

**Figure 9-3** NewTear attack




NewTear attacks cause system breakdown or restart. After defense against packet fragment attacks is enabled, the device discards all fragments of NewTear attacks.

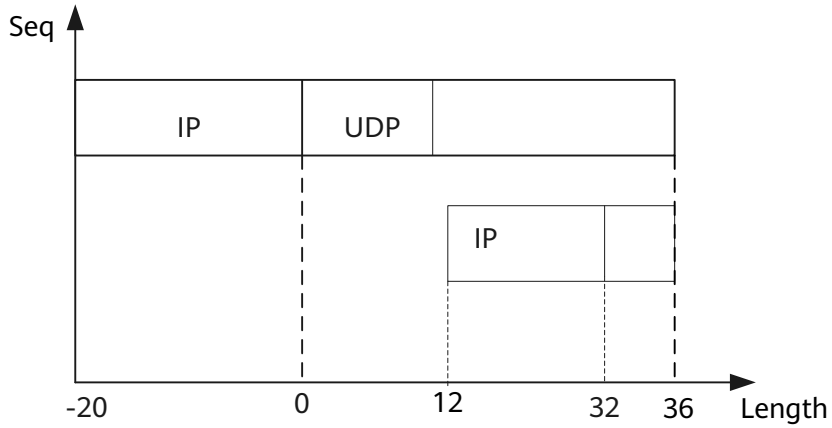
## Bonk Attack

A Bonk attack uses error fragments. As shown in **Figure 9-4**, the used protocol is UDP.

- The IP payload of the first fragment is 36 bytes including the UDP header. The UDP checksum is 0.
- The IP payload of the second fragment is 4 bytes. The offset is 32, which is incorrectly calculated. The correct offset should be 36.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 9-4** Bonk attack



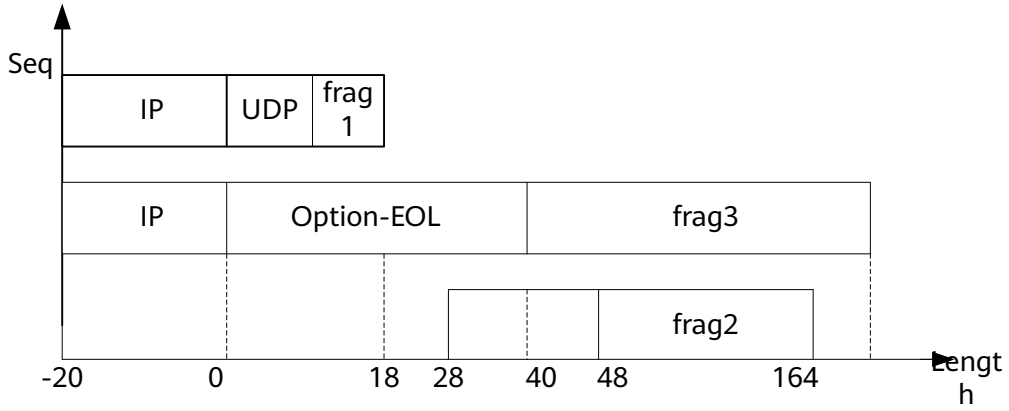

Bonk attacks cause system breakdown or restart. After defense against packet fragment attacks is enabled, the device discards all fragments in a Bonk attack.

## Nesta Attack

A Nesta attack uses error fragments. As shown in **Figure 9-5**:

- The IP payload in the first fragment is 18 bytes, the protocol used is UDP, and the checksum is 0.
- The offset in the second fragment is 48 and the IP payload is 116 bytes.
- The offset in the third fragment is 0, the **more frag** is 1 (that is, there are more fragments), the **IP option** (all EOLs) is 40 bytes, and the IP payload is 224 bytes.

**Figure 9-5** Nesta attack




Nesta attacks cause system breakdown or restart. After defense against packet fragment attacks is enabled, the device discards all fragments of Nesta attacks.

## Rose Attack

A Rose attack may utilize protocols such as UDP and TCP.

As shown in **Figure 9-6**:

If Rose attacks use TCP:

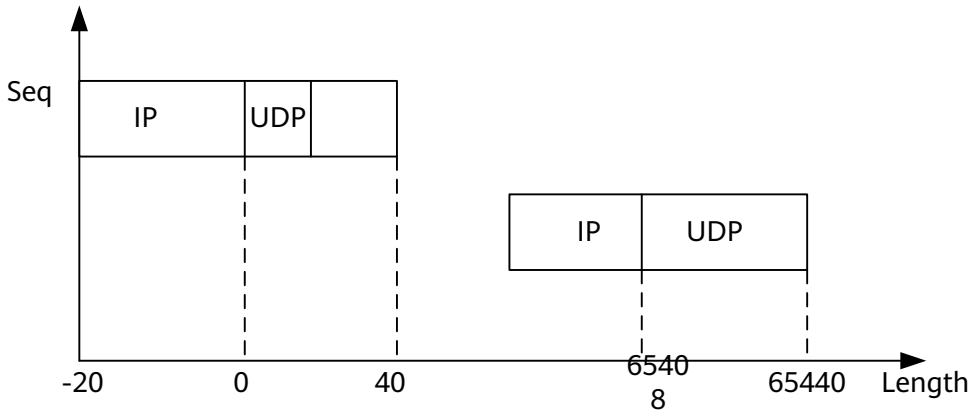

Copyright © Huawei Technologies Co., Ltd.

- The IP payload in the first fragment is 48 bytes (including the TCP header) and the length of the IP header is 20 bytes.
- The IP payload in the second fragment is 32 bytes, the offset is 65408, and the **more frag** is 0 (last fragment).

If Rose attacks use UDP:

- The IP payload in the first fragment is 40 bytes (including the UDP header, with UDP checksum 0), and the IP header is 20 bytes.
- The IP payload in the second fragment is 32 bytes, the offset is 65408, and the **more frag** is 0 (last fragment).

**Figure 9-6** Rose attack

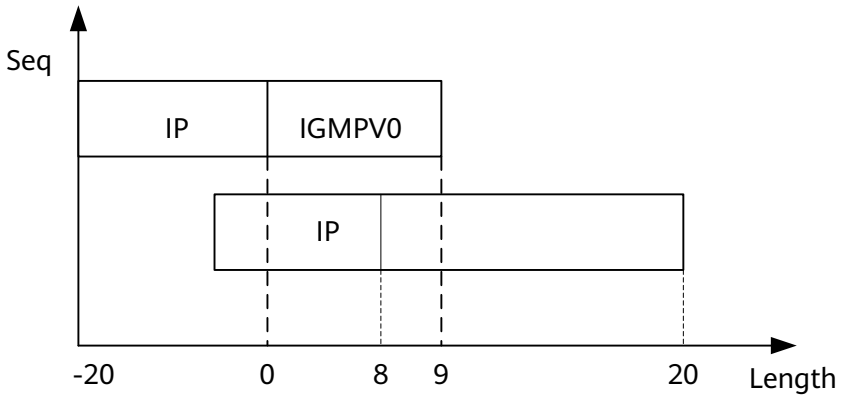



Rose attacks cause system breakdown or restart. After defense against packet fragment attacks is enabled, the device discards all fragments in a Rose attack.

## Fawx Attack

Fawx attack uses error fragments of IGMP packets. As shown in **Figure 9-7**, two fragments of an IGMP packet are sent. In the first fragment, the IP payload is 9 bytes. In the second fragment, the offset is 8, and the IP payload is 16 bytes.

**Figure 9-7** Fawx attack




Fawx attacks cause system breakdown or restart. After defense against packet fragment attacks is enabled, the device discards all fragments in a Fawx attack.

 Copyright © Huawei Technologies Co., Ltd. 

### Ping of Death Attack

An attacker sends ICMP packets with the Data field longer than 65507 bytes to attack a device. If the device processes ICMP packets that have more than 65507 bytes in the Data field, the protocol stack may crash.

After defense against packet fragment attacks is enabled, the device discards ICMP packets that have more than 65507 bytes in the Data field.

### Jolt Attack

An attacker sends packets longer than 65535 bytes to attack a device. Jolt attack uses 173 packet fragments. The IP payload of each packet fragment is 380 bytes. The total length is 65760 (173 x 380 + 20) bytes, which is greater than 65535. If the device processes such packets, the device may stop responding, crash, or restart.

After defense against packet fragment attacks is enabled, the device discards Jolt attack packets.

## 9.2.3 Defense Against Flood Attacks

If an attacker sends a large number of bogus packets to a target device, the target device is busy with these bogus packets and cannot process normal services.

Defense against flood attacks detects flood packets in real time and discards them or limits the rate of the packets to protect the device.

Flood attacks include TCP SYN flood attacks, UDP flood attacks, and ICMP flood attacks.

### TCP SYN Flood Attack

A TCP SYN flood attack uses the vulnerability of the TCP three-way handshake. During the TCP three-way handshake, the receiver sends an SYN+ACK message when receiving the first SYN message from a sender. When the receiver is waiting for the final ACK packet from the sender, the connection is in half-connected mode. If the receiver does not receive the ACK packet, the receiver retransmits a SYN+ACK packet to the sender. After several retransmission attempts, the receiver shuts down the session and then updates the session in memory. The period from the first SYN+ACK message being sent to session teardown is about 30s.

During this period, an attacker may send thousands of SYN messages to all open interfaces and does not respond to the SYN+ACK message from the receiver. This causes memory overloading on the receiver and prevents the receiver from accepting new connection requests. Then the receiver disconnects all existing connections.

After defense against TCP SYN flood attacks is enabled, the device limits the rate of TCP SYN packets to protect system resources.

### UDP Flood Attack

If an attacker sends a large number of UDP packets to a target device, the target device is busy with these UDP packets and cannot process normal services. UDP flood attacks are classified into two types:

 Copyright © Huawei Technologies Co., Ltd. 

- Fraggle attack

  An attacker sends UDP packets of which the source address is the target device's address, the destination address is the broadcast address of the target network, and the destination port is port 7. If multiple hosts use UDP echo services on the broadcast network, the target device receives excessive response packets. As a result, the system becomes busy.

  The device with attack defense configured considers packets from UDP port 7 as attack packets and discards them.
- UDP diagnosis port attack

  An attacker sends many packets to the UDP diagnosis port (7-echo, 13-daytime, and 19-Chargen) simultaneously, packets are flooded, and network devices cannot work properly.

  The device with attack defense configured considers packets from UDP ports 7, 13, and 19 as attack packets and discards them.

### ICMP Flood Attack

Generally, a network administrator monitors a network and rectifies network faults with the ping tool as follows:

1. The source host sends an ICMP Echo message to a target device.
2. When receiving the ICMP Echo message, the target device sends an ICMP Echo Reply message to the source host.

If an attacker sends many ICMP Echo messages to the target device, the target device is busy with these Echo messages and cannot process other data packets. Therefore, normal services are affected.

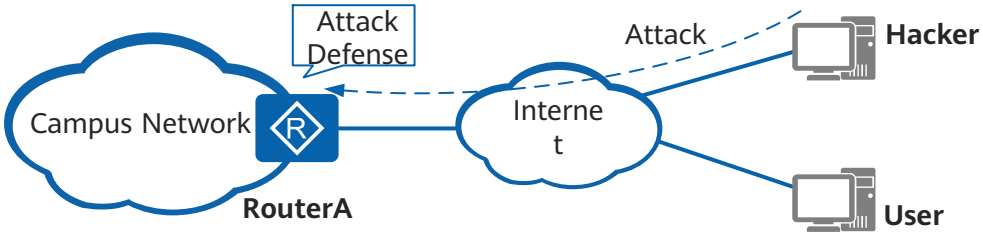
A device can use CAR to limit the rate of ICMP packets, thus protecting the CPU.

## 9.3 Application Scenarios for Attack Defense

As shown in **Figure 9-8**, when RouterA undergoes attacks, its CPU usage increases and network services are affected. To provide secure network services, the following attack defense functions are configured on RouterA:

- Preventing malformed packet attacks
- Limiting the rate of fragments to protect CPU and device resources
- Preventing flood attacks:
  - Limiting the rate of TCP SYN packets to protect the CPU
  - Discarding UDP packets sent from specified ports
  - Limiting the rate of ICMP packets to protect the CPU

**Figure 9-8** Networking diagram of attack defense




 Copyright © Huawei Technologies Co., Ltd. 

# 9.4 Licensing Requirements and Limitations for Attack Defense

## Involved Network Elements

Other network elements are not required.

## Licensing Requirements

Attack defense is a basic feature of the router and is not under license control.

## Feature Limitations

None

# 9.5 Default Settings for Attack Defense

Table 9-1 lists the default settings for attack defense.

**Table 9-1** Default settings for attack defense

| Parameter | Default Setting |
| --- | --- |
| Defense against malformed packet attacks | Enabled |
| Defense against packet fragment attacks | Enabled |
| Rate at which packet fragments are sent | 155000000 bit/s |
| Defense against TCP SYN flood attacks | Enabled |
| Rate at which TCP SYN flood packets are sent | 155000000 bit/s |
| Defense against UDP flood attacks | Enabled |
| Defense against ICMP flood attacks | Enabled |
| Rate at which ICMP flood packets are sent | 155000000 bit/s |


Copyright © Huawei Technologies Co., Ltd.

# 9.6 Configuring Defense Against Malformed Packet Attacks

## Context

Malformed packet attacks include flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits. A malformed packet attack occurs when malformed IP packets are sent to a target system, causing the system to work abnormally or break down. In addition, the attacker may send a large number of invalid packets to occupy network bandwidth.

To prevent the system from breaking down and to ensure non-stop network services, enable defense against malformed packet attacks on the device. After detecting malformed packets, the device discards them.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **anti-attack abnormal enable**

Defense against malformed packet attacks is enabled.

By default, defense against malformed packet attacks is enabled.

NOTE

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including malformed packets.

**----End**

## Verifying the Configuration

- Run the **display anti-attack statistics abnormal** command to check statistics on defense against malformed packet attacks on the device.

# 9.7 Configuring Defense Against Packet Fragment Attacks

## Context

Packet fragment attacks include attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks. If an attacker sends error packet fragments to a device, the device consumes a large number of resources to process the error packet fragments, affecting normal services.

 Copyright © Huawei Technologies Co., Ltd. 

To prevent the system from breaking down and to ensure normal network services, enable defense against packet fragment attacks on the device. The device then limits the rate of fragment packets to ensure that the CPU runs properly when the device is being attacked by many packet fragments.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **anti-attack fragment enable**

Defense against packet fragment attacks is enabled.

By default, defense against packet fragment attacks is enabled.

NOTE

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including packet fragments.

**Step 3** Run **anti-attack fragment car cir** *cir*

The rate limit of packet fragments is set.

By default, the rate limit of packet fragments is 155000000 bit/s.

**----End**

### Verifying the Configuration

- Run the **display anti-attack statistics fragment** command to check statistics on defense against packet fragment attacks on the device.

# 9.8 Configuring Defense Against Flood Attacks

## 9.8.1 Configuring Defense Against TCP SYN Flood Attacks

### Context

An attacker sends a SYN packet to a target host to initiate a TCP connection but does not respond to the SYN+ACK sent from the target host. If the target host does not receive an ACK packet from the attacker, it keeps waiting for the ACK packet. Therefore, a half-open connection is formed. If the attacker keeps sending SYN packets, the target host sets up a large number of half-open connections, thus wasting resources.

To prevent TCP SYN flood attacks, enable defense against TCP SYN flood attacks and set the rate limit for TCP SYN flood attack packets.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **anti-attack tcp-syn enable**

Defense against TCP SYN flood attacks is enabled.

By default, defense against TCP SYN flood attacks is enabled.

NOTE

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including TCP SYN flood attack packets.

**Step 3** Run **anti-attack tcp-syn car cir** *cir*

The rate limit at which TCP SYN packets are received is set.

By default, the rate limit at which TCP SYN packets are received is 155000000 bit/s.

**----End**

## 9.8.2 Configuring Defense Against UDP Flood Attacks

### Context

If an attacker sends a large number of UDP packets with specified destination port numbers to a target host in a short time, the target host is busy with these UDP packets and cannot process normal services. To prevent UDP flood attacks, enable defense against UDP flood attacks.

The device enabled with defense against UDP flood attacks discards UDP packets with port numbers 7, 13, and 19.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **anti-attack udp-flood enable**

Defense against UDP flood attacks is enabled.

By default, defense against UDP flood attacks is enabled.

NOTE

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including UDP flood attack packets.

**----End**

## 9.8.3 Configuring Defense Against ICMP Flood Attacks

### Context

If an attacker sends a large number of ICMP Echo packets to a target host in a short time, the target host is busy with these ICMP packets and cannot process

 Copyright © Huawei Technologies Co., Ltd. 

normal services. To prevent ICMP flood attacks, enable defense against ICMP flood attacks.

After defense against ICMP flood attacks is enabled, set the rate limit for ICMP flood attack packets.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **anti-attack icmp-flood enable**

Defense against ICMP flood attacks is enabled.

By default, defense against ICMP flood attacks is enabled.

NOTE

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including ICMP flood attack packets.

**Step 3** Run **anti-attack icmp-flood car cir** *cir*

The rate limit of ICMP flood attack packets is set.

By default, the rate limit of ICMP flood attack packets is 155000000 bit/s.

**----End**

## 9.8.4 Verifying the Flood Attack Defense Configuration

### Procedure

- Run the **display anti-attack statistics** [ **tcp-syn** | **udp-flood** | **icmp-flood** ] command to check statistics on defense against flood attacks.

**----End**

# 9.9 Clearing Attack Defense Statistics

### Context

NOTICE

Statistics cannot be restored after being cleared. Exercise caution when you run the reset command.

To clear attack defense statistics, run the following command.

 Copyright © Huawei Technologies Co., Ltd. 

### Procedure

- Run the **reset anti-attack statistics** [ **abnormal** | **fragment** | **tcp-syn** | **udp-flood** | **icmp-flood** ] command to clear attack defense statistics.

**----End**

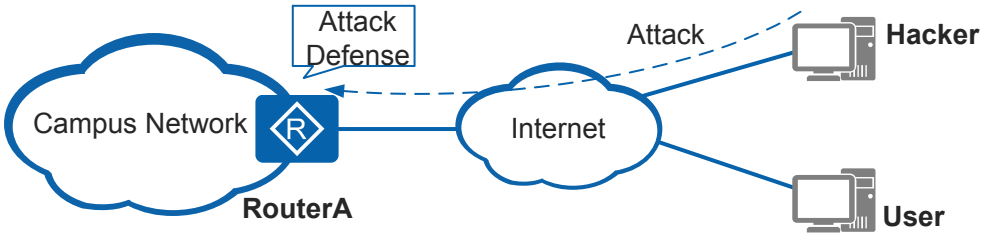
# 9.10 Configuration Examples for Attack Defense

## 9.10.1 Example for Configuring Attack Defense

### Networking Requirements

As shown in **Figure 9-9**, if a hacker on the LAN initiates malformed packet attacks, packet fragment attacks, and flood attacks to RouterA, RouterA may break down. The administrator intends to deploy attack defense measures on RouterA to provide a secure network environment and ensure normal services.

**Figure 9-9** Networking of attack defense




### Configuration Roadmap

The following configurations are performed on RouterA. The configuration roadmap is as follows:

1. Enable defense against malformed packet attacks.
2. Enable defense against packet fragment attacks.
3. Enable defense against packet flood attacks.

### Procedure

**Step 1** Enable defense against malformed packet attacks.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] anti-attack abnormal enable
```

**Step 2** Enable defense against packet fragment attacks and set the rate limit at which packet fragments are received to 15000 bit/s.

```
[RouterA] anti-attack fragment enable
[RouterA] anti-attack fragment car cir 15000
```

 Copyright © Huawei Technologies Co., Ltd. 

**Step 3** Enable defense against flood attacks.

# Enable defense against TCP SYN flood attacks and set the rate limit at which TCP SYN flood packets are received to 15000 bit/s.

```
[RouterA] anti-attack tcp-syn enable
[RouterA] anti-attack tcp-syn car cir 15000
```

# Enable defense against UDP flood attacks to discard UDP packets sent from specified ports.

```
[RouterA] anti-attack udp-flood enable
```

# Enable defense against ICMP flood attacks and set the rate limit at which ICMP flood packets are received to 15000 bit/s.

```
[RouterA] anti-attack icmp-flood enable
[RouterA] anti-attack icmp-flood car cir 15000
```

**Step 4** Verify the configuration.

# After the configuration is complete, run the **display anti-attack statistics** command to view attack defense statistics.

```
[RouterA] display anti-attack statistics
Packets Statistic Information:
-------------------------------------------------------------------------------
AntiAtkType  TotalPacketNum       DropPacketNum        PassPacketNum
           (H)       (L)       (H)       (L)       (H)       (L)
-------------------------------------------------------------------------------
Abnormal     0         0         0         0         0         0
Fragment     0         0         0         0         0         0
Tcp-syn      0         34        0         28        0         6
Udp-flood    0         0         0         0         0         0
Icmp-flood   0         0         0         0         0         0
-------------------------------------------------------------------------------
```

RouterA has statistics on discarded TCP SYN packets, indicating that the attack defense function takes effect.

**----End**

## Configuration Files

RouterA configuration file

```
#
sysname RouterA
#
anti-attack fragment car cir 15000
anti-attack tcp-syn car cir 15000
anti-attack icmp-flood car cir 15000
#
return
```

 Copyright © Huawei Technologies Co., Ltd. 

# 10 Traffic Suppression Configuration

## About This Chapter

This chapter describes basic concepts, configuration procedures, configuration examples, and common misconfigurations for traffic suppression.

10.1 Overview of Traffic Suppression

10.2 Understanding Traffic Suppression

10.3 Application Scenarios for Traffic Suppression

10.4 Licensing Requirements and Limitations for Traffic Suppression

10.5 Default Settings for Traffic Suppression

10.6 Configuring Traffic Suppression

10.7 Configuration Examples for Traffic Suppression

10.8 Troubleshooting Traffic Suppression

10.9 FAQ About Traffic Suppression

## 10.1 Overview of Traffic Suppression

### Definition

Traffic suppression can control broadcast packets, multicast packets, and unknown unicast packets and to prevent broadcast storms caused by these packets.

Traffic suppression limits the traffic by setting a threshold.

NOTE

Unknown unicast packets refer to unicast packets whose destination MAC addresses have not been learned by the device.

 Copyright © Huawei Technologies Co., Ltd. 

### Purpose

When receiving broadcast packets, multicast packets, and unknown unicast packets, the device forwards the packets to other Layer 2 Ethernet interfaces in the same VLAN if the device cannot determine the outbound interface based on the destination MAC addresses of packets. When this happens, broadcast storms may occur on the network and forwarding performance of the device will deteriorate.

Traffic suppression can control these packets and prevent broadcast storms.

# 10.2 Understanding Traffic Suppression

## 10.2.1 Traffic Suppression

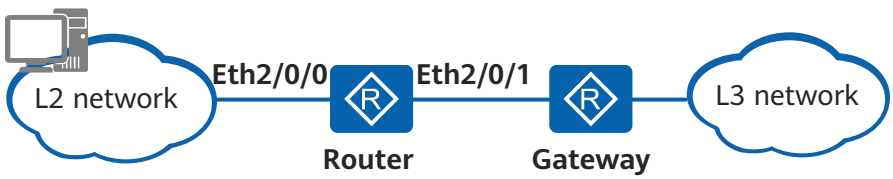
Traffic suppression prevents broadcast storms caused by broadcast packets, multicast packets, and unknown unicast packets in the following modes:

Traffic suppression is configured in the interface view to control the packets per second, and bits per second of incoming packets. The device monitors rates of these packets on the interface and compares the rates with the thresholds. When the rate of incoming traffic reaches the threshold, the system discards excess traffic.

# 10.3 Application Scenarios for Traffic Suppression

## 10.3.1 Traffic Suppression

**Figure 10-1** Networking diagram of traffic suppression




As shown in **Figure 10-1**,

- Router is connected to a Layer 2 network and a router. To limit the rates of broadcast, multicast, and unknown unicast packets forwarded by the Layer 2 network, configure traffic suppression on the Layer 2 Ethernet interface Eth2/0/0 of Router.
- You can also configure Switch A to block the outgoing broadcast, multicast, and unknown unicast packets on Eth2/0/0 to ensure Layer 2 network security.

 Copyright © Huawei Technologies Co., Ltd. 

# 10.4 Licensing Requirements and Limitations for Traffic Suppression

## Involved Network Elements

Other network elements are not required.

## Licensing Requirements

Traffic suppression is a basic feature of the router and is not under license control.

## Feature Limitations

None

# 10.5 Default Settings for Traffic Suppression

Table 10-1 lists the default settings for traffic suppression.

**Table 10-1** Default settings for traffic suppression

| Parameter | Default Setting |
| --- | --- |
| Traffic suppression on an interface | Disabled |
| Traffic suppression for Internet Control Message Protocol (ICMP) packets | Disabled |
| Traffic suppression threshold for ICMP Packets | 100 pps |

# 10.6 Configuring Traffic Suppression

## 10.6.1 Configuring Traffic Suppression on an Interface

### Context

Excess broadcast, multicast, or unknown unicast packets will cause broadcast storms. You can configure traffic suppression for a specified type of packet on an interface to limit the rate of these packets.

 Copyright © Huawei Technologies Co., Ltd. 

## Pre-configuration Tasks

Before configuring traffic suppression on an interface, configure link layer protocol parameters for interfaces to ensure that the link layer protocol status on the interfaces is Up.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface** *interface-type interface-number*

The interface view is displayed.

**Step 3** Run { **broadcast-suppression** | **multicast-suppression** | **unicast-suppression** } { **cir** *cir-value* | **packets** *packets-per-second* }

Traffic suppression is configured.

NOTE

On an AR1220E, AR1220EV, or AR1220EVW, the { **flood-suppression** | **broadcast-suppression** } **cir** *cir-value* command can only be run in the interface view to configure traffic suppression.

On an AR161EW, AR161EW-M1, AR169EW, or AR169EGW-L, the { **broadcast-suppression** | **multicast-suppression** | **unicast-suppression** } **cir** *cir-value* can only be run in the system view to configure traffic suppression.

Different types of interfaces support different modes for traffic suppression:

- The CIR value for traffic suppression can be set on the LAN-side GE interfaces and Ethernet interfaces of the main control board.
- The rate limit in pps can be set on the LAN-side GE interfaces and Ethernet interfaces of the LPU.

Different models support different types of interfaces, so the supported traffic suppression modes are different, as listed in **Table 10-2**.

**Table 10-2** Description of the supported traffic suppression modes

| Model | CIR Rate Limit | PPS Rate Limit |
| --- | --- | --- |
| AR100&AR120&AR150&AR160&AR200 series | Supported | Not supported |
| AR1200 series | Supported | Supported |
| AR2200&AR3200&AR3600 series | Not supported | Supported |

**----End**

# 10.6.2 Limiting the Rate of ICMP Packets

## Applicable Environment

The device receives a large number of ICMP packets from the network, and these packets consume a lot of CPU resources. Limiting the rate at which ICMP packets

 Copyright © Huawei Technologies Co., Ltd. 

are received can help reduce the burden of the CPU, ensuring nonstop service transmission. After this function is configured, the device discards excess packets.

NOTE

After rate limiting of ICMP packets is configured, the device may fail to respond to ping packets. To make suppression of ICMP packets take effect, disable the fast ICMP reply function.

## Procedure

- Configuring the global rate limit for ICMP packets
  a. Run **system-view**

     The system view is displayed.
  b. Run **icmp rate-limit enable**

     The global ICMP packet rate limiting function is enabled.

     By default, the global ICMP packet rate limiting function is disabled on a device.
  c. (Optional) Run **icmp rate-limit threshold** *threshold-value*

     The global rate limit for ICMP packets is set.

     By default, the global rate limit for ICMP packets is 100 pps.
- Configuring the rate limit for ICMP packets on a specified interface
  a. Run **system-view**

     The system view is displayed.
  b. Run **interface** *interface-type interface-number*

     The interface view is displayed.
  c. Run **icmp rate-limit enable**

     The ICMP packet rate limiting function is enabled on the interface.

     By default, the ICMP packet rate limiting function is disabled on a device.
  d. (Optional) Run **icmp rate-limit threshold** *threshold-value*

     The highest rate at which ICMP packets are received on the interface is set.

     By default, the rate limit for ICMP packets on an interface is 100 pps.

**----End**

# 10.6.3 Verifying the Traffic Suppression Configuration

## Procedure

- Run the **display flow-suppression interface** *interface-type interface-number* command to check the traffic suppression configuration.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

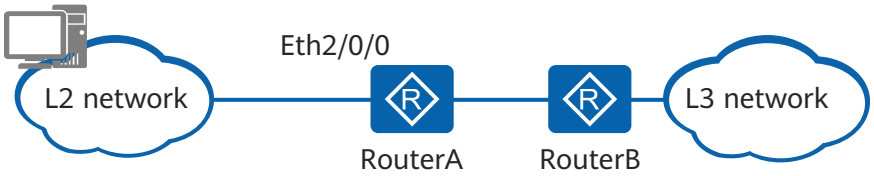
# 10.7 Configuration Examples for Traffic Suppression

## 10.7.1 Example for Setting the Rate Limit in pps for Traffic Suppression

### Networking Requirements

As shown in **Figure 10-2**, RouterA is connected to a Layer 2 network and a Layer 3 RouterB. To limit the number of broadcast, multicast, or unknown unicast packets forwarded on the Layer 2 network, you can set the rate limit in pps on Ethernet 2/0/0.

**Figure 10-2** Network diagram of Setting the Rate Limit in pps for Traffic Suppression




### Configuration Roadmap

The configuration roadmap is as follows:

- Set the rate limit in pps for traffic suppression on Ethernet 2/0/0.

### Procedure

**Step 1** Enter the interface view.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface ethernet 2/0/0
```

**Step 2** Set the rate limit in pps for broadcast packets.

```
[RouterA-Ethernet2/0/0] broadcast-suppression packets 12600
```

**Step 3** Set the rate limit in pps for multicast packets.

```
[RouterA-Ethernet2/0/0] multicast-suppression packets 25200
```

**Step 4** Set the rate limit in pps for unknown unicast packets.

```
[RouterA-Ethernet2/0/0] unicast-suppression packets 12600
[RouterA-Ethernet2/0/0] return
```

**Step 5** Verify the configuration.

Run the **display flow-suppression interface** command, and you can view the traffic suppression configuration on Ethernet 2/0/0.

```
[RouterA] display flow-suppression interface Ethernet 2/0/0
 storm type        rate mode   set rate value
```


Copyright © Huawei Technologies Co., Ltd.

```
-------------------------------------------------------------------------------
 unknown-unicast    pps          pps: 12600(packet/s)
 multicast          pps          pps: 25200(packet/s)
 broadcast          pps          pps: 12600(packet/s)
-------------------------------------------------------------------------------
```

**----End**

### Configuration Files

Configuration files on RouterA

```
#
 sysname RouterA
#
interface Ethernet2/0/0
 unicast-suppression packets 12600
 multicast-suppression packets 25200
 broadcast-suppression packets 12600
#
return
```

# 10.8 Troubleshooting Traffic Suppression

## 10.8.1 Broadcast Traffic Suppression Does Not Take Effect

### Fault Description

After broadcast traffic suppression is configured on an interface, a broadcast storm caused by broadcast packets still occurs and service traffic is interrupted.

### Common Causes

This fault is commonly caused by one of the following:

- Broadcast suppression is not configured on interfaces, or the broadcast suppression threshold is set too high.
- Broadcast packets are not discarded on the inbound interface.

NOTE

- Saving the results of each troubleshooting step is recommended. If your troubleshooting fails to correct the fault, you will have a record of your actions to provide technical support personnel.
- Troubleshooting for multicast and unknown unicast traffic suppression is similar to that for broadcast traffic suppression.

### Procedure

**Step 1** Check that traffic suppression is correctly configured on the related interface.

Run the **display flow-suppression interface** *interface-type interface-number* command in the user view to check whether the values of **rate mode** and **set rate value** in the broadcast field are proper.

 Copyright © Huawei Technologies Co., Ltd. 

- If these values are inappropriate, run the **broadcast-suppression** command to change broadcast traffic suppression parameters.
- If these values are appropriate, go to step 2.

**Step 2** Check whether broadcast packets are being discarded in the inbound direction of the interface.

Use the following methods to check whether broadcast packets are being discarded in the inbound direction of the interface:

- Run the **display interface** *interface-type interface-number* command in the user view to check whether the value of **Input bandwidth utilization** changes greatly after traffic suppression is configured. Normally, after traffic suppression is configured, bandwidth occupation on an interface decreases if the interface is discarding excess packets. If the value of **Input bandwidth utilization** does not change or changes verify little, go to step 3.
- Add another interface (interface B) to the same VLAN as the interface (interface A) that is configured with traffic suppression. Then check whether the volume of the outgoing traffic on interface B is the same as the volume of the traffic on interface A. If they are different, packets are not discarded in the inbound direction of interface A. Go to step 3.

**Step 3** Collect the following information and contact technical support personnel.

- Results of the preceding troubleshooting procedure
- Configuration file, logs, and alarms of the member switch

**----End**

# 10.9 FAQ About Traffic Suppression

## 10.9.1 Why Is the Actual Suppression Value Different from the Configured Traffic Suppression Value?

The traffic suppression supported by AR series routers is a type of granularity-based suppression.

- The AR1200 series use the committed information rate (CIR) mode.
  - If the traffic suppression value is between 64 kbit/s and 1000 kbit/s, the granularity is 64 kbit/s. For example, if the traffic suppression value is set to 65 kbit/s, the effective traffic suppression value is 64 kbit/s. If the traffic suppression value is set to 200 kbit/s, the effective traffic suppression value is 128 kbit/s, and so on.
  - If the traffic suppression value is between 1000 kbit/s and 100,000 kbit/s, the granularity is 1000 kbit/s. For example, if the traffic suppression value is set to 1001 kbit/s, the effective traffic suppression value is 1000 kbit/s. If the traffic suppression value is set to 2999 kbit/s, the effective traffic suppression value is 2000 kbit/s, and so on.
- The AR2200 and AR3200 series use the packet mode. The granularity is 125 packets per second (pps). If the traffic suppression value is set to 10 pps, the effective traffic suppression value is 0 pps. If the traffic suppression value is set to 126 pps, the effective traffic suppression value is 125 pps, and so on.

 Copyright © Huawei Technologies Co., Ltd. 

Therefore, if the traffic suppression value is not set to a multiple of the granularity, the actual suppression value is different from the traffic suppression value that is set. Within a specified granularity range, all suppression values are correct.

 Copyright © Huawei Technologies Co., Ltd. 

# 11 ARP Security Configuration

## About This Chapter

This chapter describes the principle and configuration methods of ARP security and provides configuration examples.

11.1 Overview of ARP Security

11.2 Understanding ARP Security

11.3 Application Scenarios for ARP Security

11.4 Licensing Requirements and Limitations for ARP Security

11.5 Default Settings for ARP Security

11.6 Configuring ARP Security

11.7 Maintaining ARP Security

11.8 Configuration Examples for ARP Security

11.9 FAQ About ARP Security

## 11.1 Overview of ARP Security

### Definition

Address Resolution Protocol (ARP) security prevents ARP attacks and ARP-based network scanning attacks using a series of methods such as strict ARP learning, dynamic ARP inspection (DAI), ARP anti-spoofing, and rate limit on ARP packets.

### Purpose

ARP is easy to use but lacks security protection mechanisms. Attackers may use ARP to attack network devices. The following ARP attacks exist on networks:

 Copyright © Huawei Technologies Co., Ltd. 

- ARP flood attack: ARP flood attacks, also called denial of service (DoS) attacks, occur in the following scenarios:
  - Processing ARP packets and maintaining ARP entries consume system resources. Network devices limit the number of stored ARP entries to improve ARP entry query efficiency. Attackers send a large number of bogus ARP packets with variable source IP addresses to consume ARP entries on a target device. Therefore, the target device cannot generate ARP entries when receiving ARP packets from authorized users. Consequently, communication is interrupted.
  - Attackers send a large number of IP packets with unresolvable destination IP addresses to scan the hosts on the local or remote network segments. The target devices generate many ARP Miss messages and deliver many temporary ARP entries. In addition, the target devices broadcast a large number of ARP Request packets to resolve the destination IP addresses of the IP packets received from attackers. These operations cause CPU overloading.
- ARP spoofing attack: Attackers send bogus ARP packets to target devices, causing these devices to modify the ARP entries of other network devices or user hosts. As a result, these network devices or user hosts cannot communicate with one another other.

ARP attacks cause the following problems:

- Network connections are unstable and communication is interrupted.
- Attackers initiate ARP spoofing attacks to intercept user packets and thus obtain the accounts and passwords of the users, for example, game, online banking, and file server accounts and passwords, leading to losses for customers.

To avoid the preceding problems, the device provides multiple techniques to defend against ARP attacks.

**Table 11-1** and **Table 11-2** describes various ARP security techniques for defending against different ARP attacks.

**Table 11-1** Measures to prevent ARP flood attacks

| Measure | Description | Deployment |
| --- | --- | --- |
| Rate limiting on ARP packets | Limits the rate of ARP packets to ensure that a device has sufficient CPU resources to process other services. | You are advised to enable this function on the gateway. |
| Rate limiting on ARP Miss messages | Limits the rate of ARP Miss messages to prevent attacks from a large number of IP packets with unresolvable destination IP addresses. | You are advised to enable this function on the gateway. |

 Copyright © Huawei Technologies Co., Ltd. 

| Measure | Description | Deployment |
| --- | --- | --- |
| Strict ARP learning | Allows a device to learn only ARP entries for ARP Reply packets in response to ARP Request packets that it has sent, but does not allow the device to learn the ARP entries for the ARP packets received from other devices. This prevents ARP entries from being exhausted by invalid ARP packets. | You are advised to enable this function on the gateway. |
| ARP entry limiting | Limits the total number of ARP entries that can be dynamically learned by a device's interface. This function prevents ARP entries from being exhausted when a user host connected to the interface attacks the device. | You are advised to enable this function on the gateway. |

**Table 11-2** Measures to prevent ARP spoofing attacks

| Measure | Description | Deployment |
| --- | --- | --- |
| ARP entry fixing | After a device with this function enabled learns an ARP entry for the first time, it does not modify the ARP entry, but only updates part of the entry, or sends an ARP Request packet to check the validity of the ARP packet for updating the entry. This function prevents attackers from modifying the ARP entries of authorized users by using forged ARP packets.<br>The device supports three ARP entry fixing modes: **fixed-all**, **fixed-mac**, and **send-ack**. | You are advised to enable this function on the gateway. |

 Copyright © Huawei Technologies Co., Ltd. 

| Measure | Description | Deployment |
| --- | --- | --- |
| Dynamic ARP inspection (DAI) | Allows a device to compare the source IP address, source MAC address, interface number, and VLAN ID of an ARP packet with binding entries. If an entry is matched, the device considers the ARP packet valid and allows the packet to pass through. If no entry is matched, the device considers the ARP packet invalid and discards the packet.<br>This function is available only for DHCP snooping scenarios. | You are advised to enable this function on an access device. |
| ARP gateway anti-collision | Prevents gateway ARP entries on user hosts from being modified by attackers using bogus gateway IP addresses. | You are advised to enable this function on the gateway. |
| Gratuitous ARP packet sending | Allows a gateway to periodically send ARP Request packets whose destination IP address is the device IP address to update the gateway MAC address in ARP entries. This function ensures that packets of authorized users are forwarded to the gateway and prevents hackers from intercepting these packets. | You are advised to enable this function on the gateway. |
| MAC address consistency check in an ARP packet | Prevents attacks from bogus ARP packets in which the source and destination MAC addresses are different from those in the Ethernet frame header. | You are advised to enable this function on the gateway. |
| ARP packet validity check | Allows a device to filter out packets in which the source MAC addresses are different from those in the Ethernet frame header. | You are advised to enable this function on the gateway or an access device. |

 Copyright © Huawei Technologies Co., Ltd. 

| Measure | Description | Deployment |
| --- | --- | --- |
| Strict ARP learning | Allows a device to learn only ARP entries for ARP Reply packets in response to ARP Request packets that it has sent, but does not allow the device to learn the ARP entries for the ARP packets received from other devices. This prevents the device from incorrectly updating ARP entries for the received bogus ARP packets. | You are advised to enable this function on the gateway. |

### Benefits

- Reduces maintenance costs for network operating and security.
- Provides users with stable services on a secure network.

# 11.2 Understanding ARP Security

## 11.2.1 Rate Limiting on ARP Packets

When a device is busy with a large number of ARP packets, the CPU may be incapable of processing other services. To protect CPU resources of the device, limit the rate of ARP packets.

The device provides the following measures for limiting the rate of ARP packets:

- Limiting the rate of ARP packets based on source MAC addresses or source IP addresses

  When detecting that a user host has sent a large number of ARP packets in a short period, the device limits the rate of ARP packets sent from the source MAC address or source IP address of this user host. If the number of ARP packets received per second exceeds the threshold, the device discards the excess ARP packets.

  - Limiting the rate of ARP packets based on source MAC addresses: If a MAC address is specified, the device limits the rate of ARP packets from the specified source MAC address; otherwise, the device limits the rate of ARP packets from any source MAC address.
  - Limiting the rate of ARP packets based on source IP addresses: If an IP address is specified, the device limits the rate of ARP packets from the specified source IP address; otherwise, the device limits the rate of ARP packets from any source IP address.
- Limiting the rate of ARP packets on a VLANIF interface of a super-VLAN

  A VLANIF interface of a super-VLAN is triggered to learn ARP entries in the following scenarios:

 Copyright © Huawei Technologies Co., Ltd. 

  - The VLANIF interface receives IP packets that trigger ARP Miss messages. For details about ARP Miss messages, see **11.2.2 Rate Limiting on ARP Miss Messages**.
  - The VLANIF interface enabled with ARP proxy receives ARP packets with the destination IP address matching proxy conditions but not matching any ARP entries.

  The VLANIF interface replicates ARP Request packets to each sub-VLAN when learning ARP entries. If a large number of sub-VLANs are configured for the super-VLAN, the device generates a large number of ARP Request packets. As a result, the CPU is busy processing ARP Request packets, and other services are affected. To prevent this problem, limit the rate of ARP packets on the VLANIF interface of a super-VLAN.

- Limiting the rate on ARP packets globally or on an interface

  The maximum rate and rate limiting duration of ARP packets can be set globally or on an interface. If the maximum rate and rate limiting duration are configured in the system view and interface view at the same time, the device uses the configurations in the interface view and system view in order.

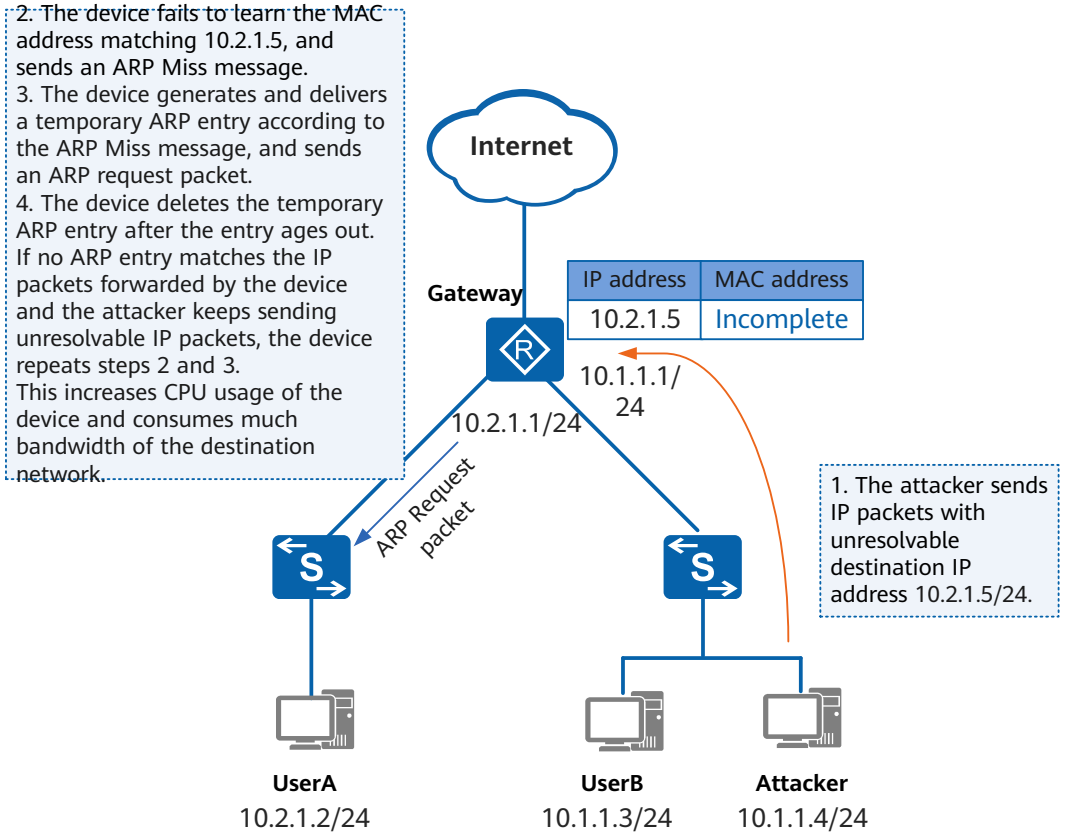
  - Limiting the rate of ARP packets globally: limits all received ARP packets.
  - Limiting the rate of ARP packets on an interface: limits the number of ARP packets processed on an interface. The configuration on an interface does not affect ARP entry learning on other interfaces.

## 11.2.2 Rate Limiting on ARP Miss Messages

When a user host sends a large number of IP packets with unresolvable destination IP addresses to attack a network device (the device has a route to the destination IP address of a packet but has no ARP entry matching the next hop of the route), the device generates a large number of ARP Miss messages. IP packets (ARP Miss packets), which trigger ARP Miss messages, are sent to the control board for processing. The device generates and delivers many temporary ARP entries according to the ARP Miss messages, and sends a large number of ARP Request packets to the destination network. This increases CPU usage of the device and consumes considerable network bandwidth. As shown in **Figure 11-1**, the attacker sends IP packets with the unresolvable destination IP address 10.2.1.5/24 to the gateway.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 11-1** ARP Miss




To avoid the preceding problems, the device takes measures to limit the rate of ARP Miss messages.

- Limiting the rate of ARP Miss messages based on source IP addresses

  If the number of ARP Miss messages triggered by IP packets and sent from a source IP address per second exceeds the limit, the device considers that an attack has been initiated by this source IP address.

  If a source IP address is specified, the rate of ARP Miss messages triggered by IP packets from this source IP address is limited. If no source IP address is specified, the rate of ARP Miss messages triggered by IP packets from any source IP address is limited.
- Limiting the rate of ARP Miss messages globally

  The device limits the number of all ARP Miss messages.
- Limiting the rate of ARP Miss messages by setting the aging time of temporary ARP entries

  When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network.

  – In the aging time of temporary ARP entries:

    ▪ Before receiving an ARP reply packet, the device discards the IP packets matching the temporary ARP entry and does not generate ARP Miss messages.

 Copyright © Huawei Technologies Co., Ltd. 

    - After receiving an ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.
  - When temporary ARP entries age out, the device clears them. If no ARP entry matches the IP packets forwarded by the device, ARP Miss messages and temporary ARP entries are repeatedly generated.

  When a device undergoes an ARP Miss attack, you can extend the aging time of temporary ARP entries and reduce the frequency of triggering ARP Miss messages to mitigate the impact on the device.

## 11.2.3 Strict ARP Learning

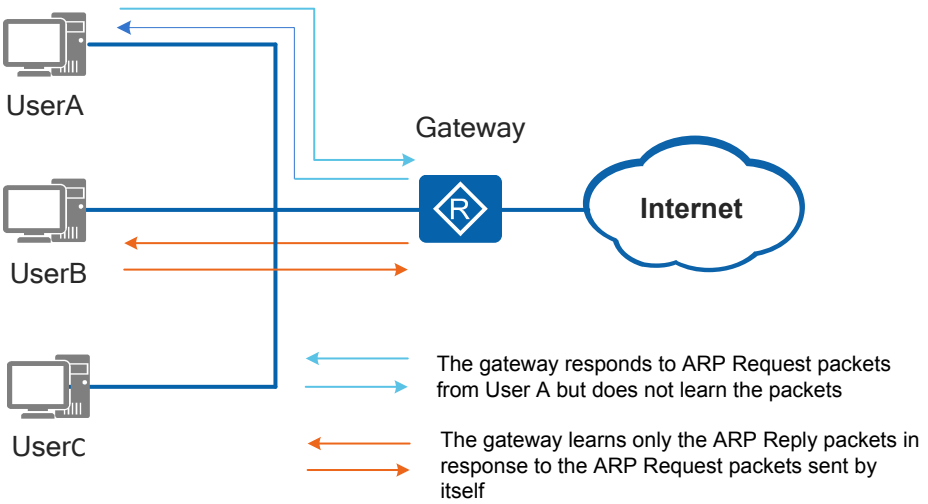
If many user hosts simultaneously send a large number of ARP packets to a device, or attackers send bogus ARP packets to the device, the following problems occur:

- Processing ARP packets consumes many CPU resources. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.
- After receiving bogus ARP packets, the device incorrectly modifies the ARP entries. As a result, authorized users cannot communicate with one another other.

To avoid the preceding problems, configure the strict ARP learning function on the gateway.

After the strict ARP learning function is enabled, the device learns only ARP entries for ARP reply packets in response to ARP Request packets that it has sent. In this way, the device can defend against most ARP attacks.

**Figure 11-2** Strict ARP learning





Copyright © Huawei Technologies Co., Ltd.

As shown in **Figure 11-2**, after receiving an ARP Request packet from UserA, the gateway sends an ARP Reply packet to UserA and adds or updates an ARP entry matching UserA. After the strict ARP learning function is enabled on the gateway:

- The gateway does not add or update an ARP entry for UserA when it receives an ARP Request packet from UserA. If the ARP Request packet requests the MAC address of the gateway, the gateway sends an ARP Reply packet to UserA.
- The gateway adds or updates an ARP entry matching UserB if it sends an ARP Request packet to UserB, after it receives the ARP Reply packet.

## 11.2.4 ARP Entry Limiting

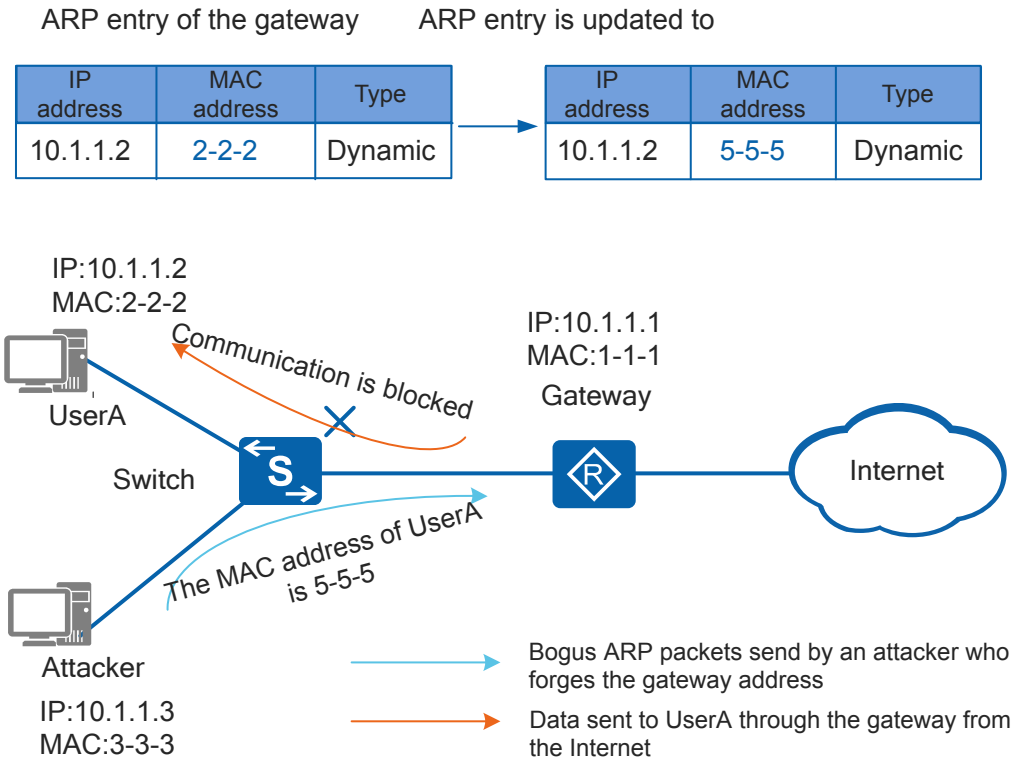
The ARP entry limiting function controls the number of ARP entries that a gateway interface can learn. By default, the number of ARP entries that an interface can dynamically learn is the same as the default number of ARP entries supported by the device. After the ARP entry limiting function is deployed, if the number of ARP entries that a specified interface dynamically learned reaches the maximum, the interface cannot learn any ARP entry. This prevents ARP entries from being exhausted when a host connecting to this interface initiates ARP attacks.

## 11.2.5 ARP Entry Fixing

As shown in **Figure 11-3**, an attacker poses as UserA to send a bogus ARP packet to the gateway. The gateway then records an incorrect ARP entry for UserA. As a result, UserA cannot communicate with the gateway.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 11-3** ARP gateway spoofing attack




To defend against ARP gateway spoofing attacks, configure the ARP entry fixing function on a gateway. After the gateway with this function enabled learns an ARP entry for the first time, it does not modify the ARP entry, but only updates part of the entry, or sends a unicast ARP Request packet to check the validity of the ARP packet for updating the entry.

The device supports three ARP entry fixing modes, as described in **Table 11-3**.

**Table 11-3** ARP entry fixing modes

| Mode | Description |
| --- | --- |
| fixed-all | When receiving an ARP packet, the device discards the packet if the MAC address, interface number, or VLAN ID does not match an ARP entry. This mode applies to networks where user MAC addresses and user access locations are fixed. |

 Copyright © Huawei Technologies Co., Ltd. 

| Mode | Description |
| --- | --- |
| fixed-mac | When receiving an ARP packet, the device discards the packet if the MAC address does not match the MAC address in the corresponding ARP entry. If the MAC address in the ARP packet matches that in the corresponding ARP entry while the interface number or VLAN ID does not match that in the ARP entry, the device updates the interface number or VLAN ID in the ARP entry. This mode applies to networks where user MAC addresses are unchanged but user access locations often change. |
| send-ack | When the device receives ARP packet A with a changed MAC address, interface number, or VLAN ID, it does not immediately update the corresponding ARP entry. Instead, the device sends a unicast ARP Request packet to the user with the IP address mapped to the original MAC address in the ARP entry, and then determines whether to change the MAC address, VLAN ID, or interface number in the ARP entry depending on the response from the user.<br>● If the device receives ARP Reply packet B within 3 seconds, and the IP address, MAC address, interface number, and VLAN ID of the ARP entry are the same as those in ARP Reply packet B, the device considers ARP packet A to be an attack packet and does not update the ARP entry.<br>● If the device does not receive an ARP Reply packet within 3 seconds or the IP address, MAC address, interface number, and VLAN ID of the ARP entry are different from those in ARP Reply packet B, the device sends a unicast ARP Request packet to the user with the IP address mapped to the original MAC address again.<br>– If the device receives ARP Reply packet C within 3 seconds, and the IP address, MAC address, interface number, and VLAN ID of the ARP packet A are the same as those in ARP Reply packet C, the device considers ARP packet A to be a valid packet and updates the ARP entry based on ARP packet A.<br>– If the device does not receive an ARP Reply packet within 3 seconds or the IP address, MAC address, interface number, and VLAN ID of ARP packet A are different from those in ARP Reply packet C, the device considers ARP packet A to be an attack packet and does not update the ARP entry.<br>This mode applies to networks where user MAC addresses and user access locations often change. |

## 11.2.6 DAI

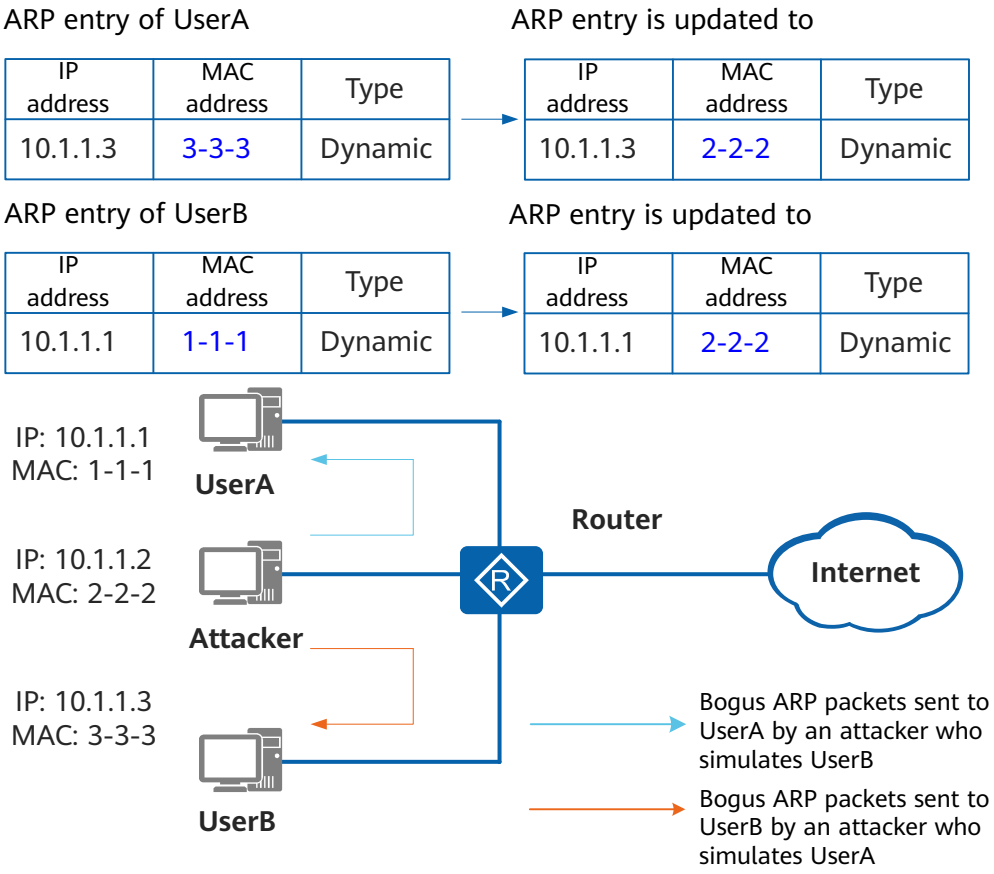

Copyright © Huawei Technologies Co., Ltd.

A man-in-the-middle (MITM) attack is a common ARP spoofing attack.

An MITM attacker establishes connections with two ends and exchanges data between them. The two ends consider that they are directly communicating, but actually the attacker has controlled the entire session. In an MITM attack, the attacker intercepts all packets going between the two ends and inserts new ones.

**Figure 11-4** shows an MITM attack scenario. An attacker poses as UserB to send a bogus ARP packet to UserA. UserA then records an incorrect ARP entry for UserB. The attacker easily obtains information exchanged between UserA and UserB. Information between UserA and UserB is not protected or secure.

**Figure 11-4** Man-in-the-middle attack




To defend against MITM attacks, configure dynamic ARP inspection (DAI) on the Router.

DAI prevents MITM attacks from using a DHCP snooping binding table. When the switch receives an ARP packet, it compares the source IP address, source MAC address, interface number, and VLAN ID of the ARP packet with binding entries. If the ARP packet matches a binding entry, the switch considers the ARP packet valid and allows the packet to pass through. If the ARP packet does not match a binding entry, the switch considers the ARP packet invalid and discards the packet.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

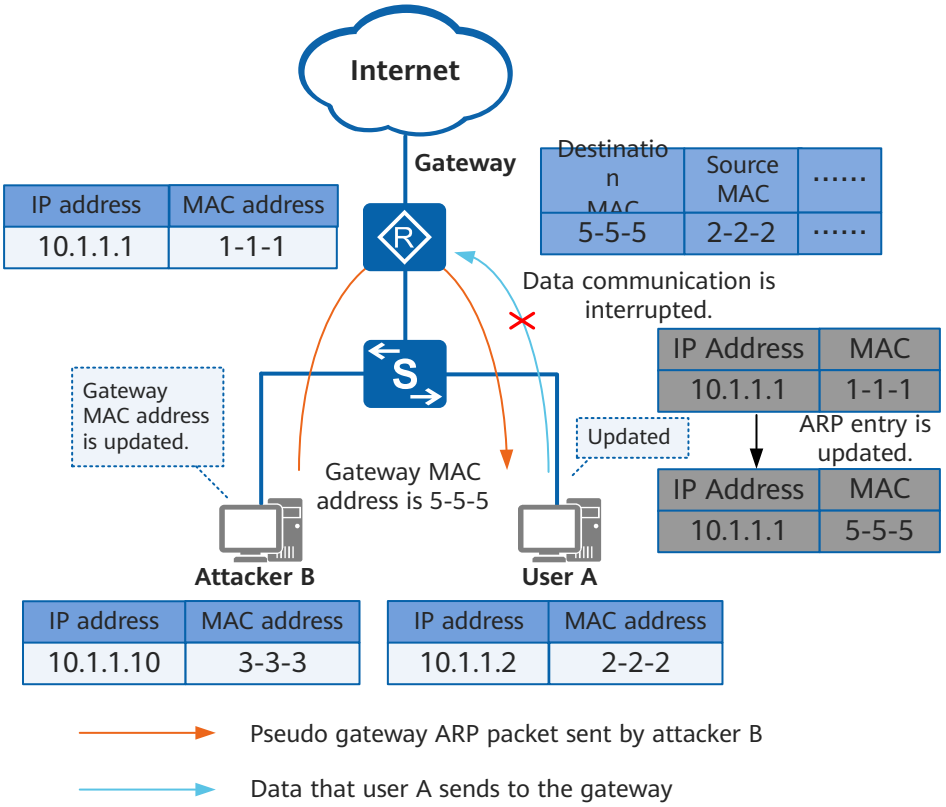
This function is available only when DHCP snooping is configured. The device enabled with DHCP snooping generates DHCP snooping binding entries when DHCP users go online. If a user uses a static IP address, you need to manually configure a static binding entry for the user. For details about DHCP snooping, see **DHCP Snooping Principle**.

When an attacker connected to the Router enabled with DAI sends bogus ARP packets, the Router detects the attacks based on the binding entries and discards the bogus ARP packets. When both the DAI and packet discarding alarm functions are enabled on the Router, the Router generates alarms when the number of discarded ARP packets matching no binding entry exceeds the alarm threshold.

## 11.2.7 ARP Gateway Anti-Collision

As shown in **Figure 11-5**, attacker B forges the gateway address to send a bogus ARP packet to user A. User A considers the attacker to be the gateway. User A then records an incorrect ARP entry for the gateway. As a result, the gateway cannot receive packets from user A and their communication is interrupted.

**Figure 11-5** ARP gateway collision




To prevent bogus gateway attacks, enable ARP gateway anti-collision on the gateway. The gateway considers that a gateway collision occurs when a received ARP packet meets either of the following conditions:

- The source IP address in the ARP packet is the same as the IP address of the VLANIF interface matching the physical inbound interface of the packet.


Copyright © Huawei Technologies Co., Ltd.

- The source IP address in the ARP packet is the virtual IP address of the inbound interface but the source MAC address in the ARP packet is not the virtual MAC address of the Virtual Router Redundancy Protocol (VRRP) group.

  NOTE

  A VRRP group, also called a virtual router, serves as the default gateway for hosts on a LAN. A virtual router has a virtual MAC address that is generated based on the virtual router ID. The virtual MAC address is in the format of 00-00-5E-00-01-{VRID}(VRRP). The virtual router sends ARP Reply packets using the virtual MAC address instead of the interface MAC address.

The device generates an ARP anti-collision entry and discards the received packets with the same source MAC address and VLAN ID in a specified period. This function prevents ARP packets with the bogus gateway address from being broadcast in a VLAN.

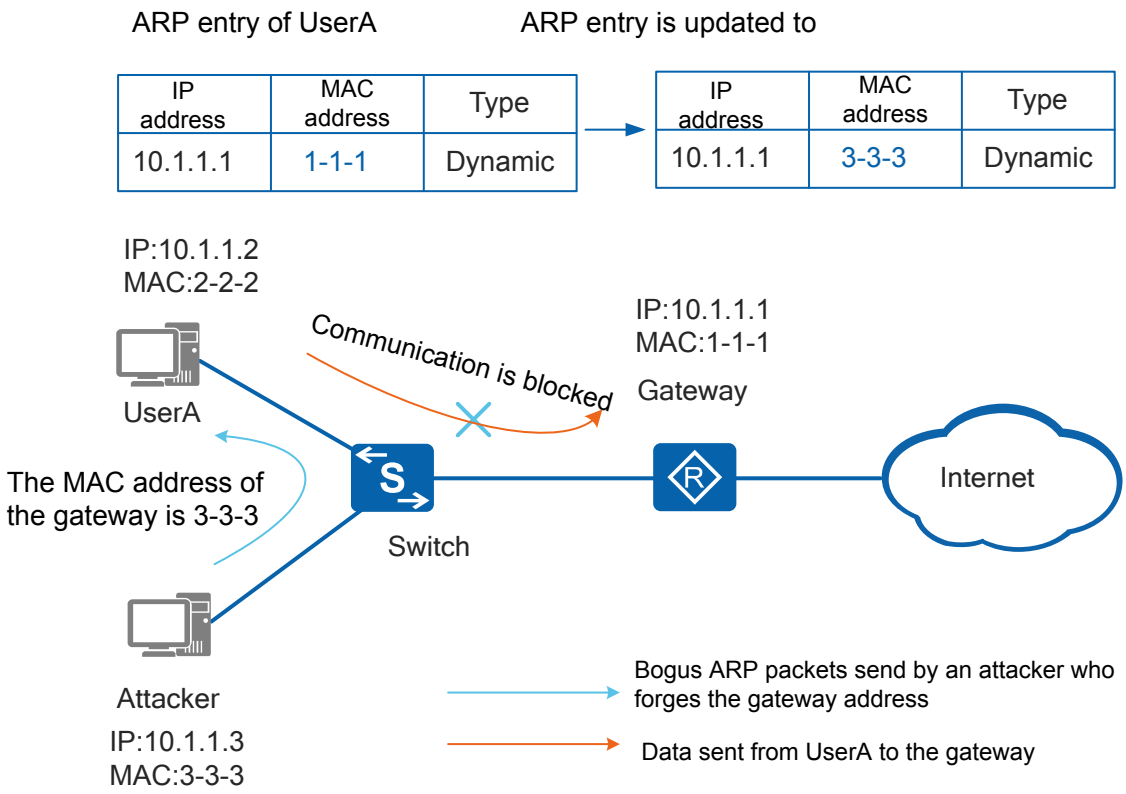
In addition, you can enable **gratuitous ARP packet sending** on the device to broadcast gratuitous ARP packets to all user hosts so that the bogus ARP entries are modified. The gratuitous ARP packet is broadcast to all users so that incorrect ARP entries are corrected.

## 11.2.8 Gratuitous ARP Packet Sending

As shown in **Figure 11-6**, an attacker forges the gateway address to send a bogus ARP packet to UserA. UserA then records an incorrect ARP entry for the gateway. As a result, the gateway cannot receive packets from UserA.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 11-6** Bogus gateway attack




To avoid the preceding problem, configure gratuitous ARP packet sending on the gateway. Then the gateway sends gratuitous ARP packets at intervals to update the ARP entries of authorized users so that the ARP entries contain the correct MAC address of the gateway.

## 11.2.9 MAC Address Consistency Check in an ARP Packet

The MAC address consistency check function for ARP packets prevents attacks from bogus ARP packets in which the source and destination MAC addresses are different from those in the Ethernet frame header. This function is usually configured on gateways.

This function enables the gateway to check the MAC address consistency in an ARP packet before ARP learning. If the source and destination MAC addresses in an ARP packet are different from those in the Ethernet frame header, the device discards the packet as an attack. If the source and destination MAC addresses in an ARP packet are the same as those in the Ethernet frame header, the device performs ARP learning.

## 11.2.10 ARP Packet Validity Check

 Copyright © Huawei Technologies Co., Ltd. 

After receiving an ARP packet, the device checks validity of the ARP packet, including:

- Packet length
- Validity of the source and destination MAC addresses in the ARP packet
- ARP Request type and ARP Reply type
- MAC address length
- IP address length
- Whether the ARP packet is an Ethernet frame

The preceding check items are used to determine whether an ARP packet is valid. The packet with different source MAC addresses in the ARP packet and Ethernet frame header is possibly an attack packet although it is allowed by the ARP protocol.

After ARP packet validity check is enabled on the gateway or an access device, the device checks the source MAC addresses in the ARP packet and Ethernet frame header, and discards the packets with inconsistent source MAC addresses.

### 11.2.11 ARP Learning Triggered by DHCP

When many DHCP users connect to a network device, the device needs to learn and maintain many ARP entries. This affects device performance.

To address this issue, configure ARP learning triggered by DHCP on the gateway. When the DHCP server allocates an IP address for a user, the gateway generates an ARP entry for the user based on the DHCP ACK packet received on the VLANIF interface. Ensure that DHCP snooping has been enabled before using ARP learning triggered by DHCP.

You can also configure DAI to prevent ARP entries of DHCP users from being modified maliciously.

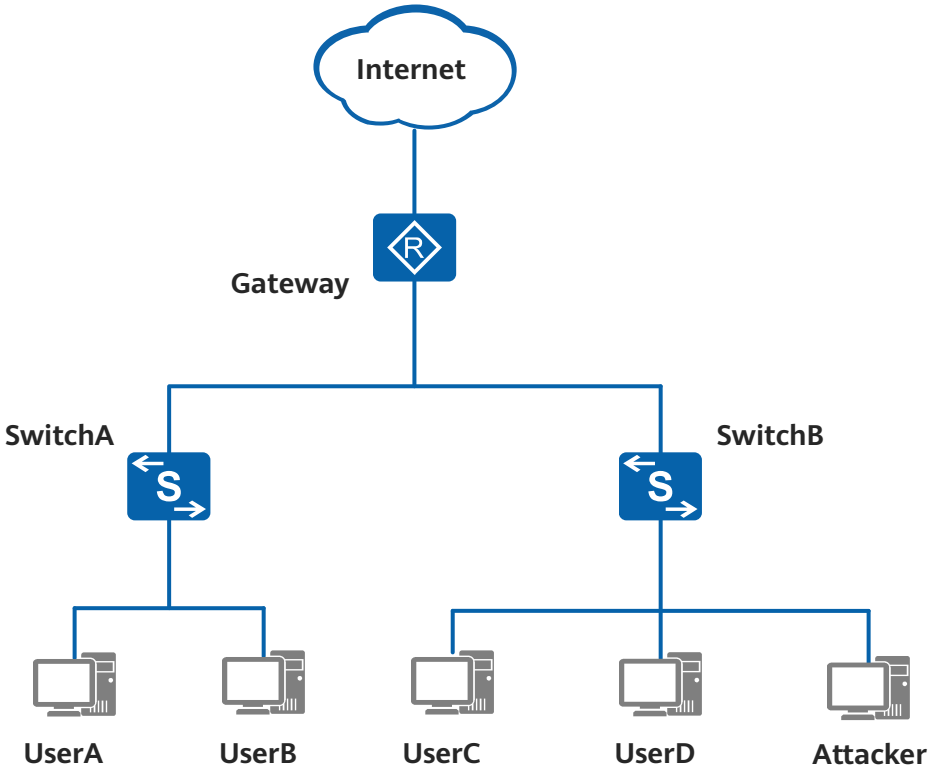
## 11.3 Application Scenarios for ARP Security

### 11.3.1 Defense Against ARP Flood Attacks

As shown in **Figure 11-7**, user hosts connect to the gateway through SwitchA and SwitchB. If a large number of ARP packets are broadcast on the network, the gateway cannot process other services due to CPU overload. Processing too many ARP packets will occupy considerable bandwidth, thus leading to network congestion and affecting network communication.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 11-7** Defending against ARP flood attacks




To avoid the preceding problems, deploy ARP flood defense functions on the gateway, including rate limit on ARP packets, rate limit on ARP Miss messages, strict ARP learning, and ARP entry limit.

- After **rate limit on ARP packets** is deployed, the gateway collects statistics on received ARP packets. If the number of ARP packets received within a specified period exceeds the threshold (the maximum number of ARP packets), the gateway discards the excess ARP packets to prevent CPU overload.
- After **rate limit on ARP Miss messages** is deployed, the gateway collects statistics on ARP Miss messages. If the number of ARP Miss messages generated within a specified period exceeds the threshold (the maximum number of ARP Miss messages), the gateway discards the IP packets triggering the excess ARP Miss messages. This prevents CPU overload when the gateway processes a large number of IP packets with unresolvable IP addresses.
- After **strict ARP learning** is deployed, the gateway learns only the ARP Reply packets in response to the ARP Request packets that it has sent. This action prevents ARP entries on the gateway from being exhausted when the gateway processes many ARP packets.
- After **ARP entry limit** is deployed, the gateway limits the number of ARP entries dynamically learned by each interface. When the number of the ARP entries dynamically learned by an interface reaches the maximum number, no more dynamic entries can be added. This prevents ARP entries from being exhausted when a host connected to the interface attacks the gateway.

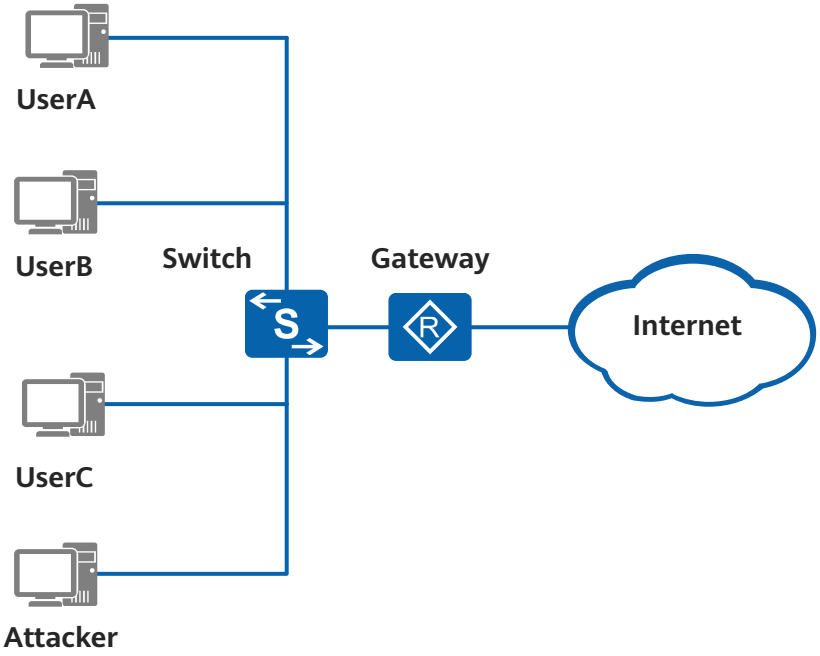
 Copyright © Huawei Technologies Co., Ltd. 

## 11.3.2 Defense Against ARP Spoofing Attacks

As shown in **Figure 11-8**, UserA, UserB, and UserC use Switch to connect to the gateway to access the Internet.

Generally, when UserA, UserB, and UserC go online and exchange ARP packets, ARP entries are created on UserA, UserB, UserC, and the gateway. At the same time, an attacker can send bogus ARP packets to UserA, UserB, UserC, or the gateway in the broadcast domain to modify ARP entries, intercept information, and interrupt communication.

**Figure 11-8** Defending against ARP spoofing attacks




To avoid the preceding problems, deploy ARP spoofing defense functions on the gateway, including rate ARP entry fixing, strict ARP learning, and gratuitous ARP packet sending.

- After **ARP entry fixing** is deployed and the gateway learns an ARP entry for the first time, the gateway does not change the ARP entry, but only updates part of the entry, or sends a unicast ARP Request packet to check the validity of the ARP packet for updating the entry. This function prevents ARP entries from being modified by bogus ARP packets.
- After **strict ARP learning** is deployed, the gateway learns only the ARP Reply packets in response to the ARP Request packets that it has sent. This prevents ARP entries from being modified by bogus ARP packets.
- After **gratuitous ARP packet sending** is deployed, the gateway periodically sends ARP Request packets with its IP address as the destination IP address to update the gateway MAC address in ARP entries. This function ensures that packets of authorized users are forwarded to the gateway and prevents hackers from intercepting these packets.


Copyright © Huawei Technologies Co., Ltd.

# 11.4 Licensing Requirements and Limitations for ARP Security

## Involved Network Elements

Other network elements are not required.

## Licensing Requirements

ARP security is a basic feature of the router and is not under license control.

## Feature imitations

None

# 11.5 Default Settings for ARP Security

Table 11-4 describes the default settings for ARP security.

**Table 11-4** Default settings for ARP security

| Parameter | Default Setting |
| --- | --- |
| Rate limit on ARP packets based on source MAC addresses | The maximum rate of ARP packets from each source MAC address is set to 0, that is, the rate of ARP packets is not limited based on the source MAC address. |
| Rate limit on ARP packets based on source IP addresses | The device allows a maximum of 5 ARP packets from the same source IP address to pass through per second. |
| Rate limit on ARP packets globally or on an interface | Disabled |
| Maximum rate and rate limiting duration of ARP packets globally or on an interface | The device allows a maximum of 100 ARP packets to pass through per second. |
| Alarm of ARP packets discarded when the rate limit is exceeded globally or on an interface | Disabled |
| Alarm threshold of ARP packets discarded when the rate limit is exceeded globally or on an interface | 100 |


Copyright © Huawei Technologies Co., Ltd.

| Parameter | Default Setting |
| --- | --- |
| Maximum rate of broadcasting ARP Request packets on the VLANIF interface of the super-VLAN | 1000 pps |
| Rate limit on ARP Miss messages based on source IP addresses | The device can process a maximum of 5 ARP Miss messages triggered by IP packets from the same source IP address. |
| Rate limit on ARP Miss messages globally | Disabled |
| Maximum rate and rate limiting duration of ARP Miss messages globally | The device can process a maximum of 100 ARP Miss messages per second. |
| Alarm of ARP Miss messages discarded when the rate limit is exceeded globally | Disabled |
| Alarm threshold of ARP Miss messages discarded when the rate limit is exceeded globally | 100 |
| Aging time of temporary ARP entries | 1 second |
| Strict ARP learning | Disabled |
| Interface-based ARP entry limit | The maximum number of ARP entries that an interface can dynamically learn is the maximum value that can be configured on the interface. |
| ARP entry fixing | Disabled |
| DAI | Disabled |
| ARP gateway anti-collision | Disabled |
| Gratuitous ARP packet sending | Disabled |
| Interval for sending gratuitous ARP packets | 90 seconds |
| MAC address consistency check in an ARP packet | Disabled |
| ARP packet validity check | Disabled |
| ARP learning triggered by DHCP | Disabled |

# 11.6 Configuring ARP Security

 Copyright © Huawei Technologies Co., Ltd. 

# 11.6.1 Configuring Defense Against ARP Flood Attacks

## Pre-configuration Tasks

Configuring defense against ARP flood attacks prevents ARP entries from being exhausted and CPU overload.

Before configuring defense against ARP flood attacks, connect interfaces and set physical parameters for the interfaces to ensure that the physical status of the interfaces is Up.

## Configuration Procedure

Operations in the configuration procedure can be performed in any sequence.

NOTE

When rate limit on ARP packets is configured globally or on an interface and rate limit on ARP packets based on the source MAC address or source IP address is also configured, the smallest rate is used.

When rate limit on ARP Miss messages is configured globally or on an interface and rate limit on ARP Miss messages based on the source IP address is also configured, the smallest rate is used.

### 11.6.1.1 Configuring Rate Limiting on ARP Packets based on Source MAC Addresses

## Context

A large number of ARP packets with a fixed source MAC address and variable IP addresses will cause the CPU of a device to be overloaded and exhaust ARP entries.

To prevent this problem, configure the gateway to limit the rate of ARP packets based on MAC addresses. The gateway then collects statistics on ARP packets sent from certain MAC addresses to the CPU. If the number of ARP packets received in one second from the specified MAC address exceeds the threshold, the device discards the excess ARP packets.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Configure rate limit on ARP packets based on source MAC addresses.

- Run **arp speed-limit source-mac maximum** *maximum*

  The maximum rate of ARP packets from any source MAC address is set

- Run **arp speed-limit source-mac** *mac-address* **maximum** *maximum*

  The maximum rate of ARP packets from the specified source MAC address is set.

 Copyright © Huawei Technologies Co., Ltd. 

When both the preceding commands are executed, the maximum rate set using the **arp speed-limit source-mac** *mac-address* **maximum** *maximum* command takes effect on ARP packets from the specified source MAC address, and the maximum rate set using the **arp speed-limit source-mac maximum** *maximum* command takes effect on ARP packets from other source MAC addresses.

By default, the maximum rate of ARP packets from each source MAC address is set to 0, that is, the rate of ARP packets is not limited based on source MAC addresses.

**----End**

### 11.6.1.2 Configuring Rate Limiting on ARP Packets based on Source IP Addresses

#### Context

When processing a large number of ARP packets with fixed IP addresses (for example, MAC addresses or outbound interfaces that match a source IP address frequently change), the CPU is overloaded and cannot process other services.

To prevent this problem, configure the gateway to limit the rate of ARP packets based on source IP addresses. The gateway collects statistics on ARP packets from a specified source IP address. If the number of ARP packets received in one second from the specified IP address exceeds the threshold, the device discards the excess ARP packets.

#### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Configure rate limit on ARP packets based on source IP addresses.

- Run **arp speed-limit source-ip maximum** *maximum*

  The maximum rate of ARP packets from any source IP address is set.
- Run **arp speed-limit source-ip** *ip-address* **maximum** *maximum*

  The maximum rate of ARP packets from the specified source IP address is set.

When both the preceding commands are executed, the maximum rate set using the **arp speed-limit source-ip** *ip-address* **maximum** *maximum* command takes effect on ARP packets from the specified source IP address, and the maximum rate set using the **arp speed-limit source-ip maximum** *maximum* command takes effect on ARP packets from other source IP addresses.

By default, the device allows a maximum of 5 ARP packets from the same source IP address to pass through per second.

**----End**

### 11.6.1.3 Configuring Rate Limiting on ARP Packets Globally or on an Interface

 Copyright © Huawei Technologies Co., Ltd. 

## Context

When processing a large number of ARP packets, a device consumes many CPU resources and cannot process other services. To protect CPU resources of the device, limit the rate of ARP packets.

After rate limiting on ARP packets is enabled, set the maximum rate and rate limiting duration of ARP packets globally or on an interface. In the rate limiting duration, if the number of received ARP packets exceeds the limit, the device discards the excess ARP packets.

- Limiting the rate of ARP packets globally: limits the number of ARP packets processed on the entire device.
- Limiting the rate of ARP packets on an interface: limits the number of ARP packets processed on an interface. The configuration on an interface does not affect ARP entry learning on other interfaces.

If the maximum rate and rate limiting duration are configured in the system view and interface view at the same time, the device uses the configurations in the interface view and system view in order.

If you want the device to generate alarms to notify the network administrator of a large number of discarded excess ARP packets, enable the alarm function. When the number of discarded ARP packets exceeds the alarm threshold, the device generates an alarm.

NOTE

If the alarm function is enabled, you need to run the **arp anti-attack log-trap-timer** *time* command to set the interval for sending alarms.

Perform the following steps on the gateway.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** (Optional) Run **interface** *interface-type interface-number*

The interface view is displayed.

NOTE

If you configure rate limiting on ARP packets in the system view, skip the preceding step.

**Step 3** Run **arp anti-attack rate-limit enable**

Rate limiting on ARP packets is enabled.

By default, rate limiting on ARP packets is disabled.

**Step 4** Run **arp anti-attack rate-limit** *packet-number* [ *interval-value* ]

The maximum rate and rate limiting duration for ARP packets are set.

By default, a maximum of 100 ARP packets are allowed to pass per second.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 5** (Optional) Run **arp anti-attack rate-limit alarm enable**

The alarm function for discarded ARP packets when the rate of ARP Miss packets exceeds the limit is enabled.

By default, the alarm function for ARP packets discarded when the rate of ARP packets exceeds the limit is disabled.

**Step 6** (Optional) Run **arp anti-attack rate-limit alarm threshold** *threshold*

The alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit is set.

By default, the alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit is 100.

**----End**

## 11.6.1.4 Configuring Rate Limiting on ARP Packets on the VLANIF Interface of a Super-VLAN

## Context

A VLANIF interface in a super-VLAN is triggered to learn ARP entries in the following scenarios:

- The VLANIF interface receives IP packets that trigger ARP Miss messages.
- The VLANIF interface is enabled with ARP proxy and receives ARP packets whose destination IP addresses meet the proxy requirements and match no ARP entry.

The VLANIF interface replicates ARP Request packets to each sub-VLAN when learning ARP entries. If a large number of sub-VLANs are configured for the super-VLAN, the device generates a large number of ARP Request packets. As a result, the CPU is busy processing ARP Request packets, and other services are affected. To prevent this problem, limit the rate of ARP packets on the VLANIF interface of a super-VLAN.

When the CPU is busy processing packets, set the maximum rate of broadcasting ARP Request packets to a small value. When the CPU is idle, set the maximum rate of broadcasting ARP Request packets to a large value. You can set the maximum rate of broadcasting ARP Request packets based on the actual network environment.

Perform the following steps on the gateway.

**NOTE**

Among the AR160 series routers, only the AR161EW, AR161EW-M1, AR169EW, and AR169EGW-L do not support Super VLAN.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 2** Run **arp speed-limit flood-rate** *rate*

The maximum rate of broadcasting ARP Request packets on VLANIF interfaces of all super-VLANs is set.

By default, the maximum rate of broadcasting ARP Request packets on VLANIF interfaces in all super-VLANs is 1000 pps.

**----End**

### 11.6.1.5 Configuring Rate Limiting on ARP Miss Messages based on Source IP Addresses

## Context

If a user host sends a large number of IP packets with unresolvable destination IP addresses to a network device (the device has a route to the destination IP address of a packet but has no ARP entry matching the next hop of the route), the device generates a large number of ARP Miss messages. IP packets triggering ARP Miss messages are sent to the device for processing. The device generates a large number of temporary ARP entries and sends many ARP Request packets to the network, consuming a large number of CPU and bandwidth resources.

If the number of ARP Miss messages triggered by IP packets from a source IP address per second exceeds the limit, the device considers that an attack has been initiated from the source IP address.

The administrator can set the maximum number of ARP Miss messages that the device can process within a specified duration based on the actual network environment, protecting the system resources and ensuring proper running of other services.

Perform the following steps on the gateway.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Configure rate limiting on ARP Miss messages based on source IP addresses.

- Run **arp-miss speed-limit source-ip maximum** *maximum*

  The maximum rate of ARP Miss messages triggered by IP packets from any source IP address is set.

- Run **arp-miss speed-limit source-ip** *ip-address* **maximum** *maximum*

  The maximum rate of ARP Miss messages triggered by IP packets from a specified source IP address is set.

When the preceding configurations are both performed, the maximum rate set using the **arp-miss speed-limit source-ip** *ip-address* **maximum** *maximum* command takes effect on ARP Miss messages triggered IP packets from the specified source IP address, and the maximum rate set using the **arp-miss speed-limit source-ip maximum** *maximum* command takes effect on ARP Miss messages triggered by IP packets from other source IP addresses.

 Copyright © Huawei Technologies Co., Ltd. 

If the maximum rate of ARP Miss messages is set to 0, the rate of ARP Miss messages is not limited based on source IP addresses. By default, the device accepts a maximum of 5 ARP Miss messages triggered by IP packets from the same source IP address per second.

**----End**

### 11.6.1.6 Configuring Rate Limiting on ARP Miss Messages Globally

## Context

If a user host sends a large number of IP packets with unresolvable destination IP addresses to a network device (the device has a route to the destination IP address of a packet but has no ARP entry matching the next hop of the route), the device generates a large number of ARP Miss messages. IP packets triggering ARP Miss messages are sent to the device for processing. The device generates a large number of temporary ARP entries and sends many ARP Request packets to the network, consuming a large number of CPU and bandwidth resources.

To avoid the preceding problems, it is recommended that you configure rate limit on ARP Miss messages on the gateway.

If you want that the device can generate alarms to notify the network administrator of a large number of discarded ARP Miss packets, enable the alarm function. When the number of discarded ARP Miss packets exceeds the alarm threshold, the device generates an alarm.

NOTE

If the alarm function is enabled, you need to run the **arp anti-attack log-trap-timer** *time* command to set the interval for sending alarms.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **arp-miss anti-attack rate-limit enable**

Rate limiting on ARP Miss messages is enabled.

By default, rate limiting on ARP Miss messages is disabled.

**Step 3** Run **arp-miss anti-attack rate-limit** *packet-number* [ *interval-value* ]

The maximum rate and rate limiting duration of ARP Miss messages are set.

By default, the device can process a maximum of 100 ARP Miss messages per second.

**Step 4** (Optional) Run **arp-miss anti-attack rate-limit alarm enable**

The alarm function for ARP Miss packets discarded when the rate of ARP Miss packets exceeds the limit is enabled.

By default, the alarm function is disabled.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 5** (Optional) Run **arp-miss anti-attack rate-limit alarm threshold** *threshold*

The alarm threshold for ARP Miss packets discarded when the rate of ARP Miss packets exceeds the limit is set.

By default, the alarm threshold is 100.

**----End**

## 11.6.1.7 Configuring the Aging Time of Temporary ARP Entries

## Context

In addition to generating ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network.

- In the aging time of temporary ARP entries:
  - Before receiving an ARP reply packet, the device discards the IP packets matching the temporary ARP entry and does not generate ARP Miss messages.
  - After receiving an ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.
- When temporary ARP entries age out, the device clears them. If no ARP entry matches the IP packets forwarded by the device, ARP Miss messages and temporary ARP entries are repeatedly generated.

You can limit the rate of ARP Miss messages by setting the aging time of temporary ARP entries. When a device undergoes an ARP Miss attack, you can extend the aging time of temporary ARP entries to reduce the frequency of triggering ARP Miss messages so that the impact on the device is minimized.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface** *interface-type interface-number*

The interface view is displayed.

The interface type can be Ethernet, GE, Eth-Trunk, or VLANIF.

**Step 3** Run **arp-fake expire-time** *expire-time*

The aging time of temporary ARP entries is set.

By default, the aging time of temporary ARP entries is 1 second.

**----End**

## 11.6.1.8 Configuring Strict ARP Learning

 Copyright © Huawei Technologies Co., Ltd. 

## Context

If many user hosts simultaneously send a large number of ARP packets to a device, or attackers send bogus ARP packets to the device, the following problems occur:

- Processing ARP packets consumes many CPU resources. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.
- After receiving bogus ARP packets, the device incorrectly modifies the ARP entries. As a result, authorized users cannot communicate with one another other.

To avoid the preceding problems, configure the strict ARP learning function on the gateway. This function allows the gateway to learn only ARP entries for ARP Reply packets in response to ARP Request packets that it has sent. In this way, the gateway can prevent most ARP attacks.

Strict ARP learning can be configured globally or in the interface view.

- If strict ARP learning is enabled globally, all interfaces on the device learn ARP entries strictly.
- If strict ARP learning is enabled in the interface view, only this interface learns ARP entries strictly.

When strict ARP learning is enabled globally and in the interface view simultaneously, the configuration on the interface takes precedence over the global configuration.

NOTE

When strict ARP learning is enabled globally:

- If you run the **arp learning strict force-disable** command on a specified interface, strict ARP learning is forced to be disabled on the interface.
- If you run the **arp learning strict trust** command on a specified interface, strict ARP learning configured globally takes effect on the interface.

## Procedure

- Configuring strict ARP learning globally
  a. Run **system-view**

     The system view is displayed.
  b. Run **arp learning strict**

     Strict ARP learning is enabled globally.

     By default, strict ARP learning is disabled.
- Configuring strict ARP learning on an interface
  a. Run **system-view**

     The system view is displayed.
  b. Run **interface** *interface-type interface-number*

     The interface view is displayed.

 Copyright © Huawei Technologies Co., Ltd. 

c. Run **arp learning strict** { **force-enable** | **force-disable** | **trust** }

Strict ARP learning on the interface is enabled.

By default, strict ARP learning is disabled on the interface.

**----End**

## 11.6.1.9 Configuring Interface-based ARP Entry Limiting

### Context

To prevent ARP entries from being exhausted by ARP attacks from a host connecting to an interface on the device, set the maximum number of ARP entries that the interface can dynamically learn. When the number of ARP entries learned by a specified interface reaches the maximum number, the interface cannot dynamically learn new ARP entries.

Perform the following steps on the gateway.

### Procedure

- Configuring ARP entry limiting on the Ethernet interface
  a. Run **system-view**

  The system view is displayed.
  b. Run **interface** *interface-type interface-number*

  The interface view is displayed.
  c. Run **arp-limit vlan** *vlan-id1* [ **to** *vlan-id2* ] **maximum** *maximum*

  ARP entry limit on the Ethernet interface is configured.

  By default, the maximum number of ARP entries that an interface can dynamically learn is the maximum value that can be configured on the interface.

  The interface type can be Ethernet, GE, VE, or Eth-Trunk. These interfaces can work at Layer 3 or Layer 2. When they work at Layer 3, you cannot configure the VLAN ID. When they work at Layer 2, you must configure the VLAN ID.
- Configuring ARP entry limit on the VLANIF interface
  a. Run **system-view**

  The system view is displayed.
  b. Run **interface vlanif** *interface-number*

  The VLANIF interface view is displayed.
  c. Run **arp-limit maximum** *maximum*

  ARP entry limit on the VLANIF interface is configured.

  By default, the maximum number of ARP entries that an interface can dynamically learn is the maximum value that can be configured on the interface.

 Copyright © Huawei Technologies Co., Ltd. 

- Configuring ARP entry limit on the sub-interface
  a. Run **system-view**

     The system view is displayed.
  b. Run **interface** *interface-type interface-number* [*.subnumber* ]

     The sub-interface view is displayed.
  c. Run **arp-limit vlan** *vlan-id1* [ **to** *vlan-id2* ] **maximum** *maximum*

     ARP entry limit on the sub-interface is configured.

     By default, the maximum number of ARP entries that an interface can dynamically learn is the maximum value that can be configured on the interface.

     The interface type can be Ethernet, GE, VE, or Eth-Trunk. These interfaces can work at Layer 3 or Layer 2. When they work at Layer 3, you cannot configure the VLAN ID. When they work at Layer 2, you must configure the VLAN ID.

**----End**

### 11.6.1.10 Verifying the ARP Flood Attack Defense Configuration

## Procedure

- Run the **display arp anti-attack configuration** { **arp-rate-limit** | **arpmiss-rate-limit** | **arp-speed-limit** | **arpmiss-speed-limit** | **entry-check** | **gateway-duplicate** | **packet-check** | **all** } command to check the ARP anti-attack configuration.
- Run the **display arp-limit** [ **interface** *interface-type interface-number* ] [ **vlan** *vlan-id* ] command to check the maximum number of ARP entries that an interface can learn.
- Run the **display arp learning strict** command to check strict ARP learning globally and on all interfaces.

**----End**

# 11.6.2 Configuring Defense Against ARP Spoofing Attacks

## Pre-configuration Tasks

If an attacker sends bogus ARP packets to a network device or user host, the device or host modifies the local ARP entries, leading to packet forwarding failures. The function of defense against ARP spoofing attacks can prevent such attacks.

Before configuring defense against ARP spoofing attacks, connect interfaces and set physical parameters for the interfaces to ensure that the physical status of the interfaces is Up.

 Copyright © Huawei Technologies Co., Ltd. 

## Configuration Procedure

Operations in the configuration procedure can be performed in any sequence.

## 11.6.2.1 Configuring ARP Entry Fixing

## Context

To defend against ARP address spoofing attacks, configure ARP entry fixing on the gateway. The **fixed-mac**, **fixed-all**, and **send-ack** modes are applicable to different scenarios and are mutually exclusive:

- **fixed-mac**: When receiving an ARP packet, the device discards the packet if the MAC address does not match that in the corresponding ARP entry. If the MAC address in the ARP packet matches that in the corresponding ARP entry while the interface number or VLAN ID does not match that in the ARP entry, the device updates the interface number or VLAN ID in the ARP entry. This mode applies to networks where user MAC addresses are unchanged but user access locations often change. When a user connects to a different interface on the device, the device updates interface information in the ARP entry of the user timely.
- **fixed-all**: When the MAC address, interface number, and VLAN ID of an ARP packet match those in the corresponding ARP entry, the device updates other information about the ARP entry. This mode applies to networks where user MAC addresses and user access locations are fixed.
- **send-ack**: When the device receives an ARP packet with a changed MAC address, interface number, or VLAN ID, it does not immediately update the corresponding ARP entry. Instead, the device sends a unicast ARP Request packet to the user with the IP address mapped to the original MAC address in the ARP entry, and then determines whether to change the MAC address, VLAN ID, or interface number in the ARP entry depending on the response from the user. This mode applies to networks where user MAC addresses and user access locations often change.

You can configure ARP entry fixing globally. If ARP entry fixing is enabled globally, all interfaces have this function enabled by default.

## Procedure

**Step 1** Configure ARP entry fixing globally

1. Run **system-view**

   The system view is displayed.

2. Run **arp anti-attack entry-check** { **fixed-mac** | **fixed-all** | **send-ack** } **enable**

   ARP entry fixing is enabled.

   By default, ARP entry fixing is disabled.

**----End**

## 11.6.2.2 Configuring DAI

 Copyright © Huawei Technologies Co., Ltd. 

## Context

Configuring DAI on an access device can prevent MITM attacks and theft on authorized users' information. After DAI is configured, the device compares the source IP address, source MAC address, VLAN ID, and interface number in the received ARP packet with binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows the packet to pass through. If the ARP packet does not match a binding entry, the device considers the ARP packet invalid and discards the packet.

You can enable DAI in the interface view or the VLAN view. When DAI is enabled in an interface view, the device checks all ARP packets received on the interface against binding entries. When DAI is enabled in the VLAN view, the device checks the ARP packets received on all interfaces belonging to the VLAN against binding entries.

If you want to receive an alarm when a large number of ARP packets are generated, enable the alarm function for the ARP packets discarded by DAI. After the alarm function is enabled, the device will generate an alarm when the number of discarded ARP packets exceeds a specified threshold.

**NOTE**

The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 board do not support DAI.

When ARP learning triggered by DHCP is enabled on the gateway, DAI can be enabled on the gateway.

This function is available only for DHCP snooping scenarios. The device enabled with DHCP snooping generates DHCP snooping binding entries when DHCP users go online. If a user uses a static IP address, you need to manually configure a static binding entry for the user. For details about the DHCP snooping configuration, see **13 DHCP Snooping Configuration**. For details on how to configure a static binding entry, see **14.6.1 Configuring IPSG Based on a Static Binding Table**.

After the DAI function is configured on the router, the port isolation and proxy ARP functions must be configured; otherwise, the DAI function does not take effect. For the configuration of port isolation, see Configuring Interface Isolation in the *Huawei AR Series Access Routers Configuration Guide - Interface Management*. For the configuration of proxy ARP, see Configuring Proxy ARP in the *Huawei AR Series Access Routers Configuration Guide - IP Services*.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface** *interface-type interface-number* or **vlan** *vlan-id*

The interface view or VLAN view is displayed.

**Step 3** Run **arp anti-attack check user-bind enable**

DAI is enabled.

By default, DAI is disabled.

**Step 4** (Optional) In the interface view, run: **arp anti-attack check user-bind check-item** { **ip-address** | **mac-address** | **vlan** }*

 Copyright © Huawei Technologies Co., Ltd. 

Or in the VLAN view, run: **arp anti-attack check user-bind check-item** { **ip-address** | **mac-address** | **interface** }*

Items for checking ARP packets based on binding entries are configured.

By default, the check items consist of IP address, MAC address, VLAN ID, and interface number.

To allow some special ARP packets that match only one or two items in binding entries to pass through, configure the device to check ARP packets according to one or two specified items in binding entries.

NOTE

Items for checking ARP packets based on binding entries do not take effect on user hosts that are configured with static binding entries. These hosts check ARP packets based on all items in static binding entries.

**Step 5** (Optional) In the interface view, run: **arp anti-attack check user-bind alarm enable**

The alarm function for ARP packets discarded by DAI is enabled.

By default, the alarm function for ARP packets discarded by DAI is disabled.

NOTICE

This type of alarm is generated for the ARP packets discarded by DAI on interfaces. Do not run the **arp anti-attack check user-bind enable** command in a VLAN and the **arp anti-attack check user-bind alarm enable** command on an interface in this VLAN at the same time; otherwise, the actual number of discarded ARP packets in the VLAN is different from the number of discarded packets on the interface.

Since the default interval for sending ARP alarms is 0 (that is, no ARP alarm is sent), you must run the **arp anti-attack log-trap-timer** *time* command to increase the alarm sending interval after enabling the alarm for packets discarded by DAI.

**Step 6** (Optional) In the interface view, run: **arp anti-attack check user-bind alarm threshold** *threshold*

The alarm threshold of ARP packets discarded by DAI is set.

By default, the threshold on an interface is consistent with the threshold set by the **arp anti-attack check user-bind alarm threshold** *threshold* command in the system view. If the alarm threshold is not set in the system view, the default threshold on the interface is 100.

**----End**

## 11.6.2.3 Configuring ARP Gateway Anti-Collision

## Context

If an attacker forges the gateway address to send ARP packets with the source IP address being the IP address of the gateway on the LAN, ARP entries on hosts in

 Copyright © Huawei Technologies Co., Ltd. 

the LAN record the incorrect gateway address. As a result, all traffic from user hosts to the gateway is sent to the attacker and the attacker intercepts user information. Communication of users is interrupted.

To prevent bogus gateway attacks, enable ARP gateway anti-collision on the gateway. The gateway considers that a gateway collision occurs when a received ARP packet meets either of the following conditions:

- The source IP address in the ARP packet is the same as the IP address of the VLANIF interface matching the physical inbound interface of the packet.
- The source IP address in the ARP packet is the virtual IP address of the inbound interface but the source MAC address in the ARP packet is not the virtual MAC address of the VRRP group.

The device generates an ARP anti-collision entry and discards the received packets with the same source MAC address and VLAN ID in a specified period. This function prevents ARP packets with the bogus gateway address from being broadcast in a VLAN.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **arp anti-attack gateway-duplicate enable**

ARP gateway anti-collision is enabled.

By default, ARP gateway anti-collision is disabled.

**----End**

## 11.6.2.4 Configuring Gratuitous ARP Packet Sending

## Context

If an attacker forges the gateway address to send ARP packets to other user hosts, ARP entries on the hosts record the incorrect gateway address. As a result, the gateway cannot receive data sent from the hosts. You can enable gratuitous ARP packet sending on the gateway. Then the gateway sends gratuitous ARP packets at intervals to update the ARP entries of authorized users so that the ARP entries contain the correct MAC address of the gateway.

You can configure gratuitous ARP packet sending globally or on a VLANIF interface.

- If gratuitous ARP packet sending is enabled globally, all interfaces have this function enabled by default.
- If gratuitous ARP packet sending is enabled globally and on a VLANIF interface simultaneously, the configuration on the VLANIF interface takes precedence over the global configuration.

## Procedure

**Step 1** Run **system-view**

 Copyright © Huawei Technologies Co., Ltd. 

The system view is displayed.

**Step 2** (Optional) Run **interface vlanif** *interface-number*

The VLANIF interface view is displayed.

NOTE

If you intend to configure gratuitous ARP packet sending in the system view, skip this step.

**Step 3** Run **arp gratuitous-arp send enable**

Gratuitous ARP packet sending is enabled.

By default, gratuitous ARP packet sending is disabled.

**Step 4** (Optional) Run **arp gratuitous-arp send interval** *interval-time*

The interval for sending gratuitous ARP packets is set.

By default, the interval for sending gratuitous ARP packets is 90 seconds.

**----End**

## 11.6.2.5 Configuring MAC Address Consistency Check in an ARP Packet

## Context

The MAC address consistency check function for ARP packets prevents attacks from bogus ARP packets in which the source and destination MAC addresses are different from those in the Ethernet frame header. This function is usually configured on gateways.

This function enables the gateway to check the MAC address consistency in an ARP packet before ARP learning. If the source and destination MAC addresses in an ARP packet are different from those in the Ethernet frame header, the device discards the packet as an attack. If the source and destination MAC addresses in an ARP packet are the same as those in the Ethernet frame header, the device performs ARP learning.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface** *interface-type interface-number*

The interface view is displayed.

**Step 3** Run **arp validate** { **source-mac** | **destination-mac** } *

MAC address consistency check in an ARP packet is enabled. This function compares the source and destination MAC addresses in ARP packets with those in the Ethernet frame header.

By default, MAC address consistency check in an ARP packet is disabled.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

Sub-interfaces do not support the **arp validate** { **source-mac** | **destination-mac** }* command. When receiving ARP packets, a sub-interface checks MAC address consistency based on the rule configured on the primary interface.

VLANIF interfaces do not support the **arp validate** { **source-mac** | **destination-mac** }* command. When receiving ARP packets, a VLANIF interface checks MAC address consistency based on the rule configured on the member interface.

**----End**

## 11.6.2.6 Configuring ARP Packet Validity Check

## Context

After receiving an ARP packet, the device checks validity of the ARP packet, including:

- Packet length
- Validity of the source and destination MAC addresses in the ARP packet
- ARP Request type and ARP Reply type
- MAC address length
- IP address length
- Whether the ARP packet is an Ethernet frame

The preceding check items are used to determine whether an ARP packet is valid. The packet with different source MAC addresses in the ARP packet and Ethernet frame header is possibly an attack packet although it is allowed by the ARP protocol.

After ARP packet validity check is enabled, the device checks the source MAC addresses in the ARP packet and Ethernet frame header, and discards the packets with inconsistent source MAC addresses.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **arp anti-attack packet-check sender-mac**

ARP packet validity check is enabled.

By default, ARP packet validity check is disabled.

**----End**

## 11.6.2.7 Configuring Strict ARP Learning

## Context

If many user hosts simultaneously send a large number of ARP packets to a device, or attackers send bogus ARP packets to the device, the following problems occur:

 Copyright © Huawei Technologies Co., Ltd. 

- Processing ARP packets consumes many CPU resources. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.
- After receiving bogus ARP packets, the device incorrectly modifies the ARP entries. As a result, authorized users cannot communicate with one another other.

To avoid the preceding problems, configure the strict ARP learning function on the gateway. This function allows the gateway to learn only ARP entries for ARP Reply packets in response to ARP Request packets that it has sent. In this way, the gateway can prevent most ARP attacks.

Strict ARP learning can be configured globally or in the interface view.

- If strict ARP learning is enabled globally, all interfaces on the device learn ARP entries strictly.
- If strict ARP learning is enabled in the interface view, only this interface learns ARP entries strictly.

When strict ARP learning is enabled globally and in the interface view simultaneously, the configuration on the interface takes precedence over the global configuration.

NOTE

When strict ARP learning is enabled globally:

- If you run the **arp learning strict force-disable** command on a specified interface, strict ARP learning is forced to be disabled on the interface.
- If you run the **arp learning strict trust** command on a specified interface, strict ARP learning configured globally takes effect on the interface.

## Procedure

- Configuring strict ARP learning globally
  a. Run **system-view**

     The system view is displayed.
  b. Run **arp learning strict**

     Strict ARP learning is enabled globally.

     By default, strict ARP learning is disabled.
- Configuring strict ARP learning on an interface
  a. Run **system-view**

     The system view is displayed.
  b. Run **interface** *interface-type interface-number*

     The interface view is displayed.
  c. Run **arp learning strict** { **force-enable** | **force-disable** | **trust** }

     Strict ARP learning on the interface is enabled.

 Copyright © Huawei Technologies Co., Ltd. 

By default, strict ARP learning is disabled on the interface.

**----End**

## 11.6.2.8 Configuring ARP Learning Triggered by DHCP

### Context

When many DHCP users connect to a network device, the device needs to learn and maintain many ARP entries. This affects device performance.

To address this issue, configure ARP learning triggered by DHCP on the gateway. When the DHCP server allocates an IP address for a user, the gateway generates an ARP entry for the user based on the DHCP ACK packet received on the VLANIF interface.

NOTE

Before configuring ARP learning triggered by DHCP, ensure that DHCP snooping is enabled using the **dhcp snooping enable** command.

When both VRRP and DHCP relay are configured on the network, neither the **dhcp snooping enable** command nor the **arp learning dhcp-trigger** command can be configured on the VRRP master and backup devices.

You can also deploy **DAI** to prevent ARP entries of DHCP users from being modified maliciously.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface vlanif** *vlan-id*

The VLANIF interface view is displayed.

**Step 3** Run **arp learning dhcp-trigger**

ARP learning triggered by DHCP is enabled.

By default, ARP learning triggered by DHCP is disabled.

**----End**

## 11.6.2.9 Verifying the ARP Spoofing Attack Defense Configuration

### Procedure

- Run the **display arp anti-attack configuration** { **arp-rate-limit** | **arpmiss-rate-limit** | **arp-speed-limit** | **arpmiss-speed-limit** | **entry-check** | **gateway-duplicate** | **packet-check** | **all** } command to check the ARP anti-attack configuration.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **display arp anti-attack check user-bind interface** *interface-type interface-number* command to check the configuration of the ARP packet check on an interface.
- Run the **display arp learning strict** command to check strict ARP learning globally and on all interfaces.
- Run the **display arp anti-attack gateway-duplicate item** command to check the ARP gateway anti-collision entries.

**----End**

# 11.7 Maintaining ARP Security

## 11.7.1 Monitoring ARP Running Status

### Procedure

- Run the **display arp packet statistics** command to display ARP packet statistics.
- Run the **display arp flood statistics** command to display statistics on ARP Request packets on VLANIF interfaces of all super-VLANs.

**----End**

## 11.7.2 Clearing ARP Security Statistics

### Context

**NOTICE**

ARP security statistics cannot be restored after being cleared. Confirm the action before you use the command.

To clear ARP security statistics, run the following commands in the user view:

### Procedure

- Run the **reset arp packet statistics** command to clear ARP packet statistics.
- Run the **reset arp flood statistics** command to clear statistics on ARP Request packets on VLANIF interfaces of all super-VLANs.
- Run the **reset arp anti-attack statistics check user-bind interface** *interface-type interface-number* command to clear statistics on ARP packets discarded for not matching binding entries.
- Run the **reset arp anti-attack statistics rate-limit** { **global** | **interface** *interface-type interface-number* } command to clear statistics on ARP packets discarded when the number of ARP packets exceeds the limit.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## 11.7.3 Configuring the Alarm Function for Potential ARP Attacks

### Context

To allow the administrator to learn the ARP running status in real time, define potential attacks, and take measures, the device provides the alarm function for potential ARP attacks. This function records exceptions of ARP running in real time. To avoid excessive alarms when ARP attacks occur, reduce the alarm quantity by setting a proper interval for sending alarms.

NOTE

The configuration takes effect only on the following alarms:

- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.4 hwARPSDaiDropALarm
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.5 hwARPGlobleSpeedLimitALarm
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.8 hwARPMissGlobleSpeedLimitALarm
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.3 hwARPSPacketCheck
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.1 hwARPSGatewayConflict
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.2 hwARPSEntryCheck

### Procedure

**Step 1** Run the **system-view** command to enter the system view.

**Step 2** Run the **arp anti-attack log-trap-timer** *time* command to set the interval for sending ARP alarms.

The default interval for sending alarms is 0, indicating that the device does not send ARP alarms.

**----End**

# 11.8 Configuration Examples for ARP Security

## 11.8.1 Example for Configuring ARP Security Functions

### Networking Requirements

As shown in **Figure 11-9**, Router connects to a server through Eth2/0/3 and connects to four users in VLAN 10 and VLAN 20 through Eth2/0/1 and Eth2/0/2. The following ARP threats exist on the network:

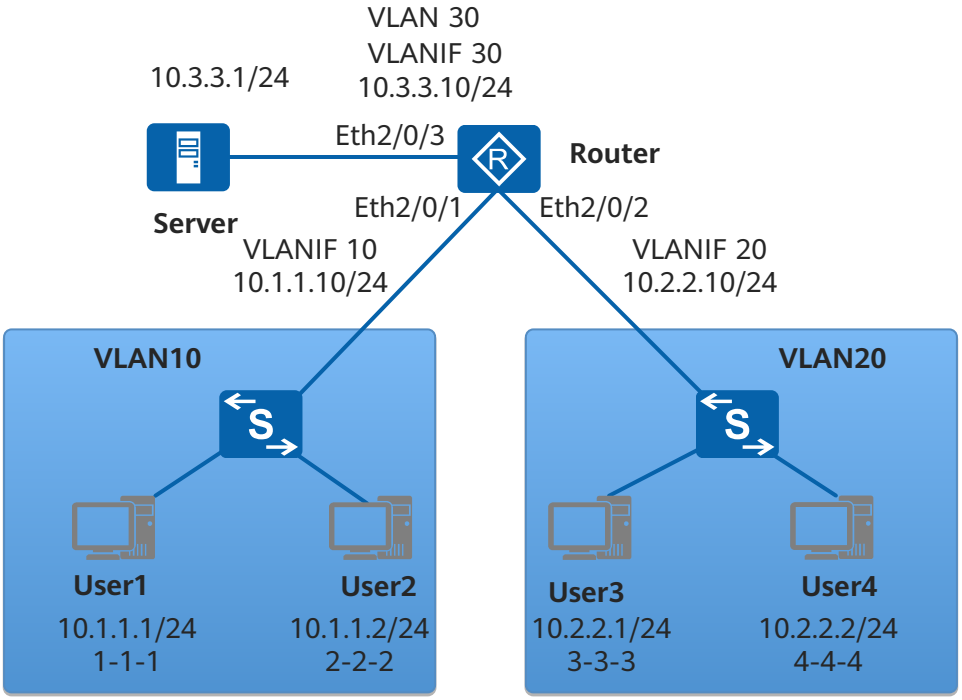
- Attackers send bogus ARP packets or bogus gratuitous ARP packets to Router. ARP entries on Router are modified, leading to packet sending and receiving failures.
- Attackers send a large number of IP packets with unresolvable destination IP addresses to Router, leading to CPU overload.

 Copyright © Huawei Technologies Co., Ltd. 

- User1 sends a large number of ARP packets with fixed MAC addresses but variable source IP addresses to Router. As a result, ARP entries on Router are exhausted and the CPU cannot process other services.
- User3 sends a large number of ARP packets with fixed source IP addresses to Router. As a result, the CPU of Router is insufficient to process other services.

The administrator wants to prevent the preceding ARP attacks and provide users with stable services on a secure network.

**Figure 11-9** Networking for configuring ARP security functions




## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure strict ARP learning and ARP entry fixing to prevent ARP entries from being modified by bogus ARP packets.
2. Configure rate limiting on ARP Miss messages based on source IP addresses. This function defends against attacks from ARP Miss messages triggered by a large number of IP packets with unresolvable IP addresses. At the same time, Router must have the capability to process a large number of ARP Miss packets from the server to ensure network communication.
3. Configure ARP entry limiting and rate limiting on ARP packets based on source MAC addresses. These functions defend against ARP flood attacks caused by a large number of ARP packets with fixed MAC addresses but variable IP addresses and prevent ARP entries from being exhausted and CPU overload.
4. Configure rate limiting on ARP packets based on source IP addresses. This function defends against ARP flood attacks from User3 with a fixed IP address and prevents CPU overload.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Create VLANs, add interfaces to the VLANs, and configure VLANIF interfaces.

# Create VLAN 10, VLAN 20, and VLAN 30, add Eth2/0/1 to VLAN 10, Eth2/0/2 to VLAN 20, and Eth2/0/3 to VLAN 30.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10 20 30
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type trunk
[Router-Ethernet2/0/1] port trunk allow-pass vlan 10
[Router-Ethernet2/0/1] quit
[Router] interface ethernet 2/0/2
[Router-Ethernet2/0/2] port link-type trunk
[Router-Ethernet2/0/2] port trunk allow-pass vlan 20
[Router-Ethernet2/0/2] quit
[Router] interface ethernet 2/0/3
[Router-Ethernet2/0/3] port link-type trunk
[Router-Ethernet2/0/3] port trunk allow-pass vlan 30
[Router-Ethernet2/0/3] quit
```

# Create VLANIF 10, VLANIF 20, and VLANIF 30, and assign IP addresses to them.

```
[Router] interface vlanif 10
[Router-Vlanif10] ip address 10.1.1.10 24
[Router-Vlanif10] quit
[Router] interface vlanif 20
[Router-Vlanif20] ip address 10.2.2.10 24
[Router-Vlanif20] quit
[Router] interface vlanif 30
[Router-Vlanif30] ip address 10.3.3.10 24
[Router-Vlanif30] quit
```

**Step 2** Configure strict ARP learning.

```
[Router] arp learning strict
```

**Step 3** Configure ARP entry fixing.

# Set the ARP entry fixing mode to **fixed-mac**.

```
[Router] arp anti-attack entry-check fixed-mac enable
```

**Step 4** Configure rate limiting on ARP Miss messages based on source IP addresses.

# Set the maximum rate of ARP Miss messages triggered by the server with the IP address 10.3.3.1 to 40 pps, and set the maximum rate of ARP Miss messages triggered by other user hosts to 20 pps.

```
[Router] arp-miss speed-limit source-ip maximum 20
[Router] arp-miss speed-limit source-ip 10.3.3.1 maximum 40
```

**Step 5** Configure interface-based ARP entry limiting.

# Configure that Eth2/0/1 can learn a maximum of 20 dynamic ARP entries.

```
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] arp-limit vlan 10 maximum 20
[Router-Ethernet2/0/1] quit
```

**Step 6** Configure rate limiting on ARP packets based on source MAC addresses.

# Set the maximum rate of ARP packets from User1 with the source MAC address 0001-0001-0001 to 10 pps.

```
[Router] arp speed-limit source-mac 0001-0001-0001 maximum 10
```

 Copyright © Huawei Technologies Co., Ltd. 

**Step 7** Configure rate limiting on ARP packets based on source IP addresses.

# Set the maximum rate of ARP packets from User3 with the source IP address 10.2.2.1 to 10 pps.

```
[Router] arp speed-limit source-ip 10.2.2.1 maximum 10
```

**Step 8** Verify the configuration.

# Run the **display arp learning strict** command to check the global configuration of strict ARP entry learning.

```
[Router] display arp learning strict
 The global configuration:arp learning strict
 Interface                       LearningStrictState
------------------------------------------------------------
------------------------------------------------------------
 Total:0
 Force-enable:0
 Force-disable:0
```

# Run the **display arp-limit** command to check the maximum number of ARP entries that the interface can dynamically learn.

```
[Router] display arp-limit interface ethernet 2/0/1
 Interface                  LimitNum   VlanID     LearnedNum(Mainboard)
--------------------------------------------------------------------------------
 Ethernet2/0/1              20         10         0
--------------------------------------------------------------------------------
 Total:1
```

# Run the **display arp anti-attack configuration all** command to check the configuration of ARP anti-attack.

```
[Router] display arp anti-attack configuration all

 ARP anti-attack packet-check function: disable

 ARP anti-attack entry-check mode: fixed-mac

 ARP gateway-duplicate anti-attack function: disabled

 ARP rate-limit configuration:
--------------------------------------------------------------------------------
 Global configuration:
 Interface configuration:
--------------------------------------------------------------------------------

 ARP miss rate-limit configuration:
--------------------------------------------------------------------------------
 Global configuration:
--------------------------------------------------------------------------------

 ARP speed-limit for source-MAC configuration:
 MAC-address         suppress-rate(pps)(rate=0 means function disabled)
--------------------------------------------------------------------------------
 0001-0001-0001   10
 Others           0
--------------------------------------------------------------------------------
 1 specified MAC addresses are configured, spec is 256 items.

 ARP speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
--------------------------------------------------------------------------------
 10.2.2.1         10
 Others           5
--------------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 256 items.
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 ARP miss speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
--------------------------------------------------------------------------------
10.3.3.1          40
Others              20
--------------------------------------------------------------------------------
1 specified IP addresses are configured, spec is 256 items.
```

# Run the **display arp packet statistics** command to check statistics on ARP-based packets.

```
[Router] display arp packet statistics
ARP Pkt Received:   sum   8678904
ARP Learnt Count:   sum     37
ARP Pkt Discard For Limit:   sum      146
ARP Pkt Discard For SpeedLimit:   sum      40529
ARP Pkt Discard For Proxy Suppress:   sum    0
ARP Pkt Discard For Other:   sum   8367601
```

In the preceding command output, the number of ARP packets discarded by Router is displayed, indicating that the ARP security functions have taken effect.

**----End**

## Configuration File

Configuration files on Router

```
#
 sysname Router
#
vlan batch 10 20 30
#
arp-miss speed-limit source-ip maximum 20
#
arp learning strict
#
arp-miss speed-limit source-ip 10.3.3.1 maximum 40
arp speed-limit source-ip 10.2.2.1 maximum 10
arp speed-limit source-mac 0001-0001-0001 maximum 10
arp anti-attack entry-check fixed-mac enable
#
interface Vlanif10
 ip address 10.1.1.10 255.255.255.0
#
interface Vlanif20
 ip address 10.2.2.10 255.255.255.0
#
interface Vlanif30
 ip address 10.3.3.10 255.255.255.0
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 arp-limit vlan 10 maximum 20
#
interface Ethernet2/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface Ethernet2/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
#
return
```

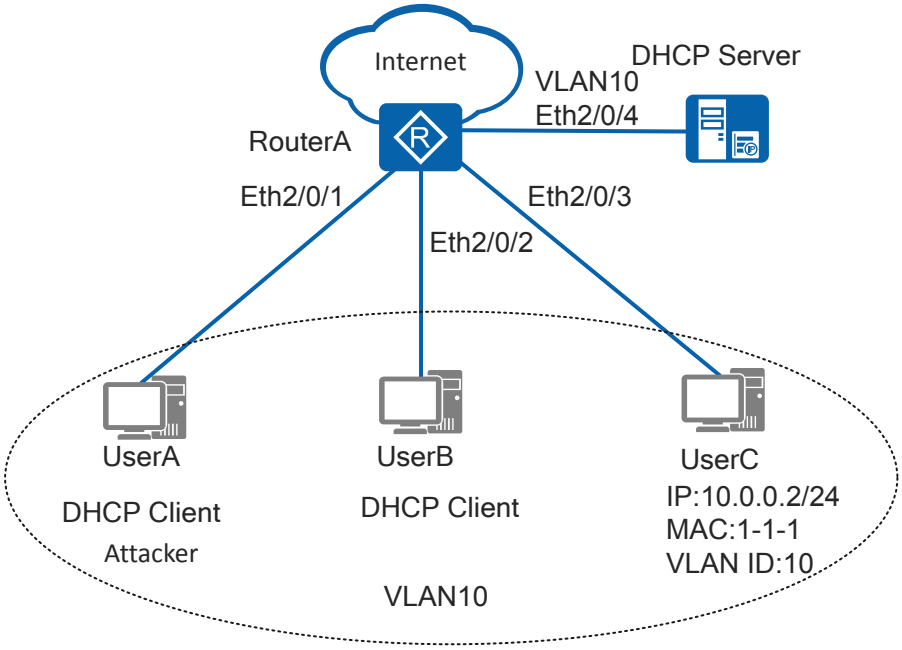
 Copyright © Huawei Technologies Co., Ltd. 

# 11.8.2 Example for Configuring Defense Against ARP MITM Attacks (All Product Models Except AR100&AR120&AR150&AR160&AR200&AR1200)

## Networking Requirements

As shown in **Figure 11-10**, the users of a department access the Internet through RouterA. Among the users connected to RouterA, some users obtain IP addresses through DHCP and some users are allocated static IP addresses. All users are in the same VLAN as the DHCP server. If attackers initiate MITM attacks, the data of authorized users will leak; therefore, the administrator requires that RouterA can prevent MITM attacks and record the frequency and range of MITM attacks.

**Figure 11-10** Networking diagram for defending against ARP MITM attacks




## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the DHCP snooping function so that RouterA can generate the address and port binding entries for dynamic users and the binding entries can be manually configured for static users. These binding entries are used for ARP packet validity check.
2. Enable DAI so that RouterA compares the source IP address, source MAC address, VLAN ID, and interface number of the ARP packet with binding entries and filter out invalid packets. This prevents ARP MITM attacks.


Copyright © Huawei Technologies Co., Ltd.

3. Enable the alarm function for the ARP packets discarded by DAI so that RouterA collects statistics on ARP packets matching no binding entry and generates alarms when the number of discarded ARP packets exceeds the alarm threshold. The administrator learns the frequency and range of the current ARP MITM attacks based on the alarms and the number of discarded ARP packets.

## Procedure

**Step 1** Create a VLAN and add interfaces to the VLAN.

# Create VLAN 10, and add Eth2/0/1, Eth2/0/2, Eth2/0/3, and Eth2/0/4 to VLAN 10.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan batch 10
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] port link-type access
[RouterA-Ethernet2/0/1] port default vlan 10
[RouterA-Ethernet2/0/1] quit
[RouterA] interface ethernet 2/0/2
[RouterA-Ethernet2/0/2] port link-type access
[RouterA-Ethernet2/0/2] port default vlan 10
[RouterA-Ethernet2/0/2] quit
[RouterA] interface ethernet 2/0/3
[RouterA-Ethernet2/0/3] port link-type access
[RouterA-Ethernet2/0/3] port default vlan 10
[RouterA-Ethernet2/0/3] quit
[RouterA] interface ethernet 2/0/4
[RouterA-Ethernet2/0/4] port link-type trunk
[RouterA-Ethernet2/0/4] port trunk allow-pass vlan 10
[RouterA-Ethernet2/0/4] quit
```

**Step 2** Configure DHCP snooping.

# Enable DHCP snooping globally.

```
[RouterA] dhcp enable
[RouterA] dhcp snooping enable
```

# Enable DHCP snooping in VLAN 10.

```
[RouterA] vlan 10
[RouterA-vlan10] dhcp snooping enable
[RouterA-vlan10] quit
```

# Configure Eth2/0/4 as a trusted interface.

```
[RouterA] interface ethernet 2/0/4
[RouterA-Ethernet2/0/4] dhcp snooping trusted
[RouterA-Ethernet2/0/4] quit
```

**Step 3** Configure a static binding table.

```
[RouterA] user-bind static ip-address 10.0.0.2 mac-address 0001-0001-0001 interface ethernet 2/0/3 vlan 10
```

**Step 4** Enable DAI and the packet discarding alarm function.

# Eth2/0/1 is used as an example. The configurations of Eth2/0/1, Eth2/0/2, and Eth2/0/3 are similar to the configuration of Eth2/0/1, and are not mentioned here.

```
[RouterA] interface ethernet 2/0/1
[RouterA-Ethernet2/0/1] arp anti-attack check user-bind enable
[RouterA-Ethernet2/0/1] arp anti-attack check user-bind alarm enable
[RouterA-Ethernet2/0/1] quit
```

 Copyright © Huawei Technologies Co., Ltd. 

**Step 5** Verify the configuration.

# Run the **display arp anti-attack check user-bind interface** command to check the DAI configuration on each interface. Eth2/0/1 is used as an example.

```
[RouterA] display arp anti-attack check user-bind interface ethernet 2/0/1
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 ARP packet drop count = 966
```

In the preceding command output, the number of discarded ARP packets on Eth2/0/1 is displayed, indicating that the defense against ARP MITM attacks has taken effect.

When you run the **display arp anti-attack check user-bind interface** command for multiple times on each interface, the administrator can learn the frequency and range of ARP MITM attacks based on the value of **ARP packet drop count**.

**----End**

## Configuration File

Configuration file of RouterA

```
#
sysname RouterA
#
vlan batch 10
#
dhcp enable
#
dhcp snooping enable
user-bind static ip-address 10.0.0.2 mac-address 0001-0001-0001 interface Ethernet2/0/3 vlan 10
#
vlan 10
 dhcp snooping enable
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
#
interface Ethernet2/0/2
 port link-type access
 port default vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
#
interface Ethernet2/0/3
 port link-type access
 port default vlan 10
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
#
interface Ethernet2/0/4
 port link-type trunk
 port trunk allow-pass vlan 10
 dhcp snooping trusted
#
return
```

# 11.9 FAQ About ARP Security

 Copyright © Huawei Technologies Co., Ltd. 

## 11.9.1 After I Enable ARP Gateway Anti-Collision, and Send Gateway Collision ARP Packets from a MAC Address, Why Can the MAC Address Not Forward Traffic?

After the Address Resolution Protocol (ARP) anti-collision function detects gateway collision ARP packets, the system prohibits the source media access control (MAC) address from forwarding packets for three minutes.

## 11.9.2 After I Send ARP Request Packets with the Same Source IP Address, Why Do I Sometimes Receive Response Packets Only at the Rate of 5 Packets Per Second?

By default, AR series routers limit the rate of Address Resolution Protocol (ARP) packets with the same source IP address to prevent ARP attacks. The default rate limit is 5 packets per second.

## 11.9.3 How Do I Take Measures to Prevent Internal Network Attacks?

Internal network attacks refer to attacks from Layer 2 protocol packets. Attacks often use ARP to attack network devices. ARP attack defense measures are often used:

- Strict ARP learning: The device learns only the ARP Reply packets in response to the ARP Request packets sent by itself. Run the **arp learning strict** command to enable strict ARP learning.
- ARP gateway anti-collision: If an attacker sends an ARP packet with the source IP address as the gateway address, ARP entries are modified incorrectly. ARP gateway anti-collision can solve this problem. Run the **arp anti-attack gateway-duplicate enable** command to enable the ARP gateway anti-collision function.
- Sending gratuitous ARP packets: To ensure that packets sent by hosts on the internal network are forwarded to the gateway or prevent malicious users from intercepting these packets, the device sends gratuitous ARP packets at intervals to update the gateway address in ARP entries of the hosts. Run the **arp gratuitous-arp send enable** command to enable the device to send gratuitous ARP packets. By default, the device sends gratuitous ARP packets every 90s.

**NOTE**

If too many security measures are used, device performance may deteriorate.

 Copyright © Huawei Technologies Co., Ltd. 

# 12 Port Security Configuration

## About This Chapter

This chapter describes how to configure port security on Huawei devices.

12.1 Overview of Port Security

12.2 Understanding Port Security

12.3 Application Scenarios for Port Security

12.4 Licensing Requirements and Limitations for Port Security

12.5 Default Settings for Port Security

12.6 Configuring Port Security

12.7 Configuration Examples for Port Security

## 12.1 Overview of Port Security

Port security changes the dynamic MAC addresses learned on an interface into secure MAC addresses (including dynamic and sticky MAC addresses). Only hosts using secure MAC addresses or static MAC addresses can communicate with the device through the interface. This function enhances device security.

## 12.2 Understanding Port Security

A device takes certain actions after the number of secure MAC addresses reaches the limit.

### Classification of Secure MAC Addresses

Secure MAC addresses fall into dynamic secure MAC addresses and sticky MAC addresses.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 12-1** Classification of secure MAC addresses

| Type | Description | Characteristic |
| --- | --- | --- |
| Dynamic secure MAC address | MAC addresses that are learned on an interface where port security is enabled but the sticky MAC address function is disabled. | Dynamic secure MAC addresses will be lost after a device restart and need to be learned again.<br>Dynamic secure MAC addresses will never be aged out by default, and can be aged only when an aging time is set for them. |
| Sticky MAC address | MAC addresses that are learned on an interface where both port security and sticky MAC address function are enabled. | Sticky MAC addresses are not aged out. The sticky MAC addresses that are saved manually are not lost after a device restart. |

Before port security is enabled on an interface, MAC address entries can be configured statically or learned dynamically on the interface. After port security is enabled on an interface, dynamic MAC address entries that have been learned on the interface are deleted and MAC address entries learned subsequently turn into secure dynamic MAC address entries. Only packets with source MAC addresses matching the secure dynamic MAC address entries or static MAC address entries can pass through the interface. After the sticky MAC address function is enabled on the interface, existing secure dynamic MAC address entries and MAC address entries learned subsequently on the interface turn into sticky MAC address entries. When the number of secure MAC addresses reaches the limit, the switch stops learning MAC addresses on the interface and takes a protection action on the interface or packets received.

## Action to Take After the Number of Secure MAC Addresses Reaches the Limit

If the switch receives packets with a nonexistent source MAC address after the number of secure MAC addresses reaches the limit, the switch considers that the packets are sent from an unauthorized user and takes the configured action on the interface. By default, the switch discards the packets and generates an alarm in such a situation.

**Table 12-2** Port security actions

| Action | Description |
| --- | --- |
| restrict | Discards packets with a nonexistent source MAC address and generates an alarm. This action is recommended.<br>**NOTE**<br>When receiving packets with a nonexistent source MAC address, the switch generates at least one alarm and at most two alarms every 30 seconds. |

 Copyright © Huawei Technologies Co., Ltd. 

| Action | Description |
| --- | --- |
| protect | Only discards packets with a nonexistent source MAC address but does not generate an alarm. |
| shutdown | Sets the interface state to error-down and generates an alarm.<br>By default, an interface cannot automatically restore to Up state after it is shut down. To restore the interface, run the **undo shutdown** command on the interface in sequence. Alternatively, run the **restart** command on the interface to restart the interface. |

# 12.3 Application Scenarios for Port Security

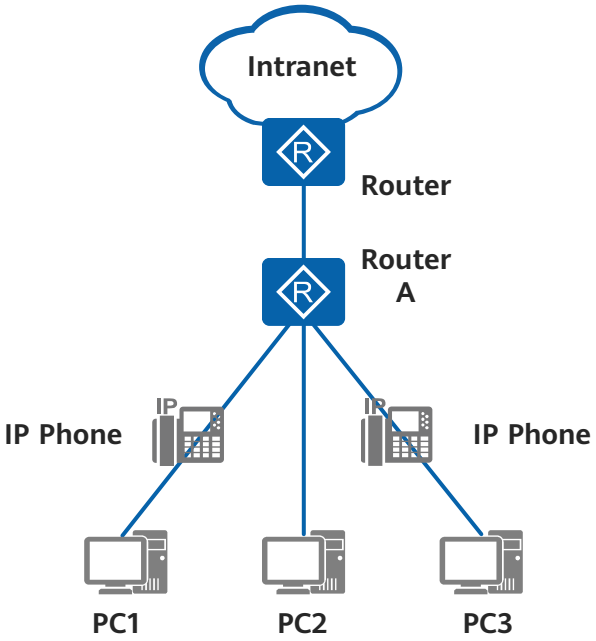
Port security usually applies to the following scenarios:

- The access device configured with port security can defend against attacks initiated by an unauthorized user using another interface.
- The aggregation device configured with port security can limit the number of access users.

## Configuring Port Security at the Access Layer

As shown in Figure 12-1, PC1 and PC3 connect to RouterA using IP phones, and PC2 directly connects to RouterA. To ensure access device security and defend against attacks from unauthorized users, configure port security on the interface of RouterA.

**Figure 12-1** Configuring port security at the access layer





Copyright © Huawei Technologies Co., Ltd.

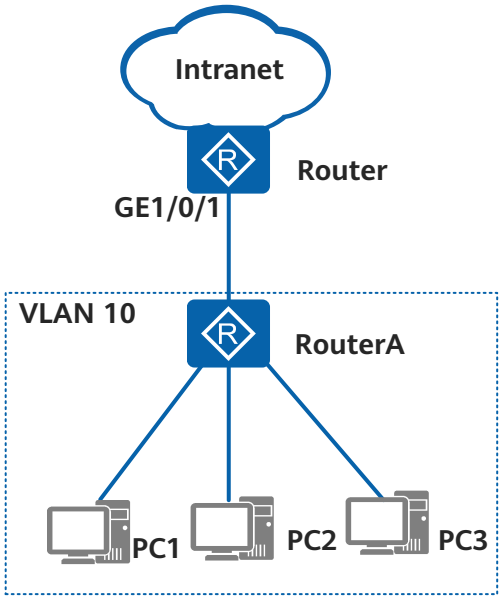
NOTE

- If access users frequently change the locations, you can configure port security to convert dynamic MAC addresses into dynamic secure MAC addresses. This function ensures that bound MAC address entries are deleted immediately when users change the locations.
- If access users seldom change the locations, you can configure port security to convert dynamic MAC addresses into sticky MAC addresses. This function ensures that bound MAC address entries are not lost after a device reset.

### Configuring Port Security at the Aggregation Layer

As shown in **Figure 12-2**, multiple PCs communicate with the switch through RouterA on a tree network. To ensure aggregation device security and limit the number of access users, configure port security on the aggregation device Router and set the maximum number of secure MAC addresses.

**Figure 12-2** Configuring port security at the aggregation layer




## 12.4 Licensing Requirements and Limitations for Port Security

### Involved Network Elements

Other network elements are not required.

### Licensing Requirements

Port security is a basic feature of the router and is not under license control.

### Feature Limitations

When deploying port security on the router, pay attention to the following:

 Copyright © Huawei Technologies Co., Ltd. 

- An interface can learn only one secure MAC address by default. Set the maximum number of secure MAC addresses according to actual networking.
- The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support port security.
- The AR100&AR120 series, AR161G-L, AR169-P-M9, AR161, AR161W, AR169, AR169G-L, AR169W, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR161G-U, AR169RW-P-M9, AR169W-P-M9, AR2204-24GE, AR2204-51GE, AR2204-48GE-P, AR169CVW, AR161EW-M1, AR169EGW-L, AR161G-Lc, AR169CVW-4B4S, AR161EW, AR169EW do not support port security.

# 12.5 Default Settings for Port Security

**Table 12-3** Default settings for port security

| Parameter | Default Setting |
| --- | --- |
| Port security | Disabled |
| Maximum number of secure MAC addresses learned by an interface | 1 |
| Action to take after the number of learned secure MAC addresses reaches the limit | restrict: discards packets with a nonexistent source MAC address and generates an alarm |
| Aging time of secure MAC address entries | Not aged |

# 12.6 Configuring Port Security

Port security changes the dynamic MAC addresses learned on an interface into secure MAC addresses (including dynamic and sticky MAC addresses). This function prevents unauthorized users from communicating with the router using this interface and therefore enhances device security.

## Pre-configuration Tasks

Before configuring port security, complete the following tasks:

- Disable MAC address limiting on the interface.
- Disable MUX VLAN.
- Disable MAC address authentication.
- Disable 802.1x authentication.
- Disable MAC address security for DHCP snooping on the interface.

 Copyright © Huawei Technologies Co., Ltd. 

# 12.6.1 Configuring the Secure MAC Address Function

## Context

You can configure port security on networks demanding high access security. Port security enables the router to convert MAC addresses learned by an interface into secure MAC addresses and to stop learning new MAC addresses after the maximum number of learned MAC addresses is reached. In this case, the router can only communicate with devices with learned MAC addresses. This prevents devices with untrusted MAC addresses from communicating with the router through this interface, improving security of the device and network.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface** *interface-type interface-number*

The interface view is displayed.

**Step 3** Run **port-security enable**

Port security is enabled.

By default, port security is disabled on an interface.

**Step 4** Run **port-security max-mac-num** *max-number*

The maximum number of secure MAC addresses learned by an interface is set.

By default, the maximum number of secure MAC addresses learned by an interface is 1.

NOTE

- An interface can learn only one secure MAC address by default. If multiple PCs connect to the company network using one interface, run the **port-security max-mac-num** command to change the maximum number of secure MAC addresses.
- If a PC connects to the router using an IP phone, set the maximum number of secure MAC addresses to 3 because the IP phone occupies two MAC address entries and the PC occupies one MAC address entry. The VLAN IDs in two MAC address entries used by the IP phone are different. The two VLANs are used to transmit voice and data packets respectively.

**Step 5** (Optional) Run **port-security protect-action** { **protect** | **restrict** | **shutdown** }

A port security action is configured.

By default, the **restrict** action is used.

**Step 6** (Optional) Run **port-security aging-time** *time*

The aging time of dynamic secure MAC address entries learned by the interface is set.

 Copyright © Huawei Technologies Co., Ltd. 

By default, dynamic secure MAC address entries learned by an interface are not aged out.

**----End**

## Follow-up Procedure

- Check secure MAC addresses.

  Run the **display mac-address security** [ **vlan** *vlan-id* | *interface-type interface-number* ] command to check dynamic secure MAC address entries.
- If the router receives packets with a nonexistent source MAC address after the number of secure MAC addresses reaches the limit, the router considers that the packets are sent from an unauthorized user and takes the configured action on the interface. There are three actions: restrict, protect, and shutdown.

  **Table 12-4** Port security actions

| Action | Description |
| --- | --- |
| restrict | Discards packets with a nonexistent source MAC address and generates an alarm. This action is recommended.<br>**NOTE**<br>When receiving packets with a nonexistent source MAC address, the switch generates at least one alarm and at most two alarms every 30 seconds. |
| protect | Only discards packets with a nonexistent source MAC address but does not generate an alarm. |
| shutdown | Sets the interface state to error-down and generates an alarm.<br>By default, an interface cannot automatically restore to Up state after it is shut down. To restore the interface, run the **undo shutdown** command on the interface in sequence. Alternatively, run the **restart** command on the interface to restart the interface. |

# 12.6.2 Configuring the Sticky MAC Address Function

## Context

You can configure port security on networks demanding high access security. Port security enables the router to convert MAC addresses learned by an interface into secure MAC addresses and to stop learning new MAC addresses after the maximum number of learned MAC addresses is reached. In this case, the router can only communicate with devices with learned MAC addresses. This prevents devices with untrusted MAC addresses from communicating with the router through this interface, improving security of the device and network.

The sticky MAC address function usually applies to networks where terminal users seldom change.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface** *interface-type interface-number*The interface view is displayed.

**Step 3** Run **port-security enable**

Port security is enabled.

By default, port security is disabled on an interface.

**Step 4** Run **port-security mac-address sticky**

The sticky MAC address function is enabled on the interface.

By default, the sticky MAC address function is disabled on an interface.

**Step 5** Run **port-security max-mac-num** *max-number*

The maximum number of sticky MAC addresses is set.

By default, an interface enabled with the sticky MAC address function can learn only one sticky MAC address.

NOTE

- An interface can learn only one secure MAC address by default. If multiple PCs connect to the company network using one interface, run the **port-security max-mac-num** command to change the maximum number of secure MAC addresses.
- If a PC connects to the router using an IP phone, set the maximum number of secure MAC addresses to 3 because the IP phone occupies two MAC address entries and the PC occupies one MAC address entry. The VLAN IDs in two MAC address entries used by the IP phone are different. The two VLANs are used to transmit voice and data packets respectively.

**Step 6** (Optional) Run **port-security protect-action** { **protect** | **restrict** | **shutdown** }

A port security action is configured.

By default, the **restrict** action is used.

**Step 7** (Optional) Run **port-security mac-address sticky** *mac-address* **vlan** *vlan-id*

A sticky MAC address entry is configured.

NOTE

- After the sticky MAC address function is enabled on an interface, existing dynamic secure MAC address entries and MAC address entries learned subsequently on the interface turn into sticky MAC address entries.
- After the sticky MAC address function is enabled on an interface, sticky MAC address entries are not aged even if the **port-security aging-time** command is configured.
- The saved sticky MAC address entries are not lost after a device restart.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

### Follow-up Procedure

- Run the **display mac-address sticky** [ **vlan** *vlan-id* | *interface-type interface-number* ] command to check sticky MAC address entries.
- If the switch receives packets with a nonexistent source MAC address after the number of secure MAC addresses reaches the limit, the switch considers that the packets are sent from an unauthorized user and takes the configured action on the interface. There are three actions: restrict, protect, and shutdown.

**Table 12-5** Port security actions

| Action | Description |
| --- | --- |
| restrict | Discards packets with a nonexistent source MAC address and generates an alarm. This action is recommended.<br>**NOTE**<br>When receiving packets with a nonexistent source MAC address, the switch generates at least one alarm and at most two alarms every 30 seconds. |
| protect | Only discards packets with a nonexistent source MAC address but does not generate an alarm. |
| shutdown | Sets the interface state to error-down and generates an alarm.<br>By default, an interface cannot automatically restore to Up state after it is shut down. To restore the interface, run the **undo shutdown** command on the interface in sequence. Alternatively, run the **restart** command on the interface to restart the interface. |

# 12.7 Configuration Examples for Port Security

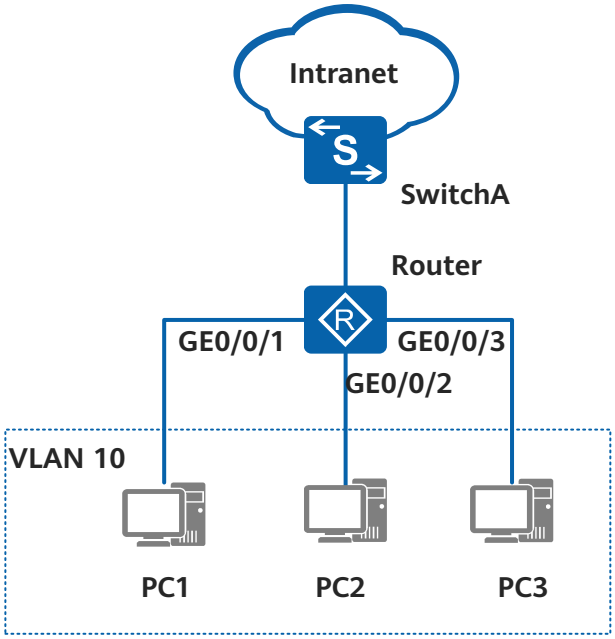
## 12.7.1 Example for Configuring Port Security

### Networking Requirements

As shown in **Figure 12-3**, PC1, PC2, and PC3 connect to the company network through the router. For high user access security, port security is enabled on the interface of the router and the maximum number of MAC addresses to be learned on the interface is set to the number of access users so that external users cannot use their PCs to access the company network.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 12-3** Networking for configuring port security




## Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN to implement Layer 2 forwarding.
2. Configure port security so that learned MAC address entries are not aged out.

## Procedure

**Step 1** Create a VLAN on the router and add interfaces to the VLAN.

# Create a VLAN.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan 10
[Router-vlan10] quit
```

# Add GE0/0/1 to VLAN 10. The configurations of GE0/0/2 and GE0/0/3 are similar to the configuration of GE0/0/1, and are not mentioned here.

```
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] port link-type access
[Router-GigabitEthernet0/0/1] port default vlan 10
[Router-GigabitEthernet0/0/1] quit
```

**Step 2** Configure port security on GE0/0/1.

# Enable the sticky MAC address function and set the maximum number of MAC addresses. The configurations of GE0/0/2 and GE0/0/3 are similar to the configuration of GE0/0/1, and are not mentioned here.

```
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] port-security enable
[Router-GigabitEthernet0/0/1] port-security mac-address sticky
[Router-GigabitEthernet0/0/1] port-security max-mac-num 1
```

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

- An interface can learn only one secure MAC address by default. If multiple PCs connect to the company network using one interface, run the **port-security max-mac-num** command to change the maximum number of secure MAC addresses.
- If a PC connects to the router using an IP phone, set the maximum number of secure MAC addresses to 3 because the IP phone occupies two MAC address entries and the PC occupies one MAC address entry. The VLAN IDs in two MAC address entries used by the IP phone are different. The two VLANs are used to transmit voice and data packets respectively.

**Step 3** Verify the configuration.

If PC1, PC2, and PC3 are replaced by other PCs, the PCs cannot access the company network.

**----End**

## Configuration Files

Router configuration file

```
#
 sysname Router
#
vlan batch 10
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
 port-security enable
 port-security mac-address sticky
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 10
 port-security enable
 port-security mac-address sticky
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 10
 port-security enable
 port-security mac-address sticky
#
return
```

 Copyright © Huawei Technologies Co., Ltd. 

# 13 DHCP Snooping Configuration

## About This Chapter

13.1 Overview of DHCP Snooping
13.2 Understanding DHCP Snooping
13.3 Application Scenarios for DHCP Snooping
13.4 Licensing Requirements and Limitations for DHCP Snooping
13.5 Default Settings for DHCP Snooping
13.6 Configuring Basic Functions of DHCP Snooping
13.7 Configuring DHCP Snooping Attack Mitigation
13.8 Inserting the Option 82 Field in a DHCP Message
13.9 Configuring the LDRA to Detect Client Locations
13.10 Inserting the Option 18 or Option 37 Field in a DHCPv6 Message
13.11 Maintaining DHCP Snooping
13.12 Configuration Examples for DHCP Snooping
13.13 Troubleshooting DHCP Snooping
13.14 FAQ About DHCP Snooping

## 13.1 Overview of DHCP Snooping

### Definition

The Dynamic Host Configuration Protocol (DHCP) snooping feature ensures that DHCP clients obtain IP addresses only from authorized DHCP servers and a DHCP snooping-enabled device records mappings between IP addresses and MAC addresses of DHCP clients, preventing DHCP attacks on the network.

 Copyright © Huawei Technologies Co., Ltd. 

### Purpose

DHCP defined in RFC 2131 is susceptible to certain attacks, such as a bogus DHCP server attack, DHCP server DoS attack, and bogus DHCP message attack.

DHCP snooping functions as a firewall between DHCP clients and the DHCP server to prevent DHCP attacks on the network, facilitating security for communication services.

### Benefits

- A DHCP snooping-enabled device can defend against DHCP attacks on the network. This enhances device reliability and network stability.
- Service stability and network security are improved.

# 13.2 Understanding DHCP Snooping

## 13.2.1 DHCP Snooping Fundamentals

DHCP snooping provides the trusted interface and listening functions.

### Trusted Interface

DHCP snooping involves two interface roles: trusted interface and untrusted interfaces, through which DHCP snooping ensures that DHCP clients obtain IP addresses from a valid DHCP server.

If a bogus DHCP server exists on a network, DHCP clients may obtain incorrect IP addresses and network configuration parameters from it, leading to communication failures. The trusted interface controls the source of DHCP Reply messages to prevent bogus DHCP servers from assigning IP addresses and other configurations to other DHCP clients.

Trusted interface and untrusted interfaces process DHCP messages as follows:

- The device receives DHCP ACK messages, NAK messages, and Offer messages through the trusted interface.
- The device discards DHCP ACK messages, NAK messages, and Offer messages on untrusted interfaces.

NOTE

The administrator configures the interface directly or indirectly connected to an authorized DHCP server as the trusted interface, and other interfaces as untrusted interfaces. This ensures that DHCP clients obtain IP addresses from authorized DHCP servers.

### Listening

After DHCP snooping is enabled, the device generates a DHCP snooping binding table by listening to DHCP Request messages and Reply messages. A binding entry contains the MAC address, IP address, interface number, and Virtual Local Area Network (VLAN) ID of the DHCP client.

 Copyright © Huawei Technologies Co., Ltd. 

The DHCP snooping binding entries are aged out when the DHCP release expires, or the entries are deleted when users send DHCP Release packets to release IP addresses.

The administrator needs to record IP addresses of DHCP clients and identify the mappings between the IP addresses and MAC addresses of the DHCP clients. The DHCP snooping binding table helps the administrator conveniently record the mappings.

The DHCP snooping binding table records the mapping between IP addresses and MAC addresses of DHCP clients. The device can check DHCP messages against the DHCP snooping binding table to prevent attacks initiated by unauthorized users.

To ensure that the device obtains parameters such as MAC addresses for generating a DHCP snooping binding table, configure DHCP snooping on the Layer 2 access devices or the first DHCP relay agent from the device to the DHCP server.

## 13.2.2 Option 82 Supported by DHCP Snooping

### Overview

In the traditional method of dynamically allocating IP addresses, a DHCP server cannot determine the DHCP client location from the received DHCP Request message. As a result, DHCP clients in the same VLAN have the same rights to access network resources. This brings challenges in security control because the network administrator cannot control network access of clients in the same VLAN.

RFC 3046 defines the DHCP Relay Agent Information Option (Option 82), which records the location of a DHCP client. A DHCP snooping-enabled device or a DHCP relay agent inserts the Option 82 field into a DHCP Request message to notify the DHCP server of the DHCP client location. In this case, the DHCP server assigns an IP address and other configurations to the DHCP client, implementing security control over the DHCP client.

The Option 82 field contains two commonly used suboptions: circuit ID and remote ID. The circuit ID distinguishes the VLAN ID and interface number of a client, and the remote ID distinguishes the MAC address of the device to which the client connects.

When functioning as a DHCP relay agent, a device supports the Option 82 field regardless of whether DHCP snooping is enabled. However, when functioning as an access device on a Layer 2 network, the device supports the Option 82 field only after DHCP snooping is enabled.

The Option 82 field records only the location of a DHCP client and is encapsulated in a DHCP Request message sent to the DHCP server. To deploy different IP address assignment or security policies for different clients, the DHCP server must support the Option 82 field and be configured with IP address assignment or security policies.

The Option 82 field is different from parameters recorded in a DHCP snooping binding table. The device adds the Option 82 field to the DHCP Request message when a DHCP client requests an IP address (at this time, the client does not have an IP address). However, a DHCP snooping binding entry is generated based on

 Copyright © Huawei Technologies Co., Ltd. 

the DHCP ACK messages received from the DHCP server (at this time, an IP address has been assigned to the client).

### Implementation

A device uses the following modes to insert the Option 82 field into a DHCP Request message:

- Insert mode: Upon receiving a DHCP Request message without the Option 82 field, the device inserts the Option 82 field. If the DHCP Request message contains the Option 82 field, the device checks whether the Option 82 field contains a remote ID. If a remote ID is present, the device retains the Option 82 field. Otherwise, the device inserts a remote ID.
- Rebuild mode: Upon receiving a DHCP Request message without the Option 82 field, the device inserts the Option 82 field. If the DHCP Request message contains the Option 82 field, the device deletes the original Option 82 field and inserts the Option 82 field set by the administrator.

The device handles reply messages from the DHCP server in the same way regardless of whether the Insert or Rebuild mode is used.

- If the DHCP Request messages received by the device do not contain the Option 82 field, the device deletes the Option 82 field from the DHCP Reply messages and then forwards them to the DHCP client.
- If the DHCP Request messages contain the Option 82 field, the device changes the Option 82 format in the DHCP Reply messages to that in the DHCP Request messages and then forwards the reply messages to the DHCP client.
- If the DHCP Reply messages do not contain the Option 82 field, the device directly forwards the messages.

## 13.2.3 LDRA Supported by DHCPv6 Snooping

### Overview

A Lightweight DHCPv6 Relay Agent (LDRA), defined in RFC 6221, is used to insert relay agent options in DHCPv6 exchange messages to identify user locations.

Similar to Option 82 in DHCPv4, the LDRA provides user location information in DHCPv6. Generally, the LDRA is configured on the client-side access devices.

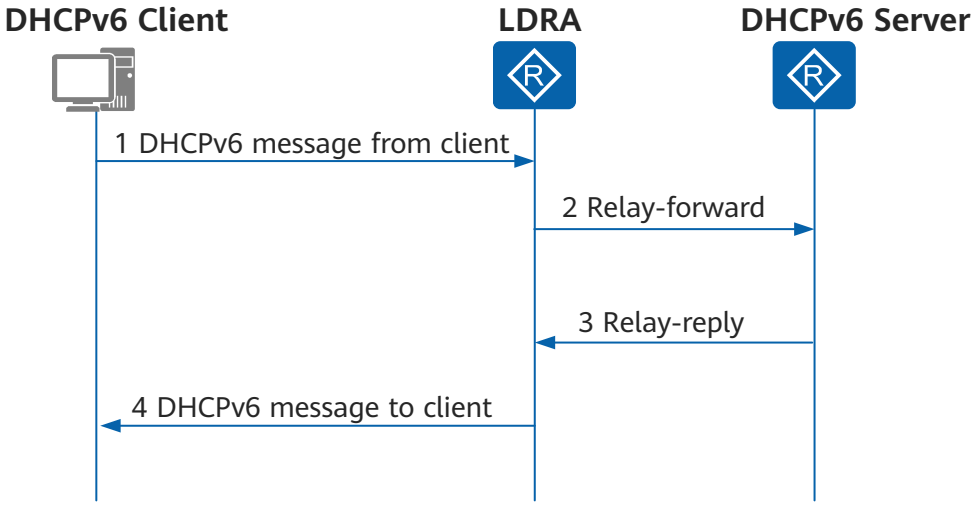
### Implementation

The working mechanism of an LDRA is similar to that of a DHCPv6 relay agent. When receiving a DHCPv6 request from a client, the LDRA-enabled device encapsulates client location information (such as the information about the interface connecting the client and the device) in a Relay-Forward message, and forwards the message to the DHCPv6 server. The DHCPv6 server obtains the location information of the client, and accordingly assigns an IP address, QoS policy, and access control policy to the client.

**Figure 13-1** shows the LDRA interaction process.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 13-1** LDRA interaction process




1. A DHCPv6 client sends a DHCPv6 request message to the LDRA-enabled device.
2. The LDRA-enabled device encapsulates the request message into the relay agent option and the location information of the client into the interface-id or remote-id option in a Relay-Forward message and forwards the message to the DHCPv6 server.
3. The DHCPv6 server obtains the request message and location information of the client from the Relay-Forward message. The server then selects an IPv6 address and other parameters for the client, constructs a reply, encapsulates the reply into a Relay-Reply message, and sends the Relay-Reply message to the LDRA-enabled device.
4. The LDRA-enabled device obtains the reply from the Relay-Reply message, and forwards the reply to the DHCPv6 client. The client then obtains the address of the DHCPv6 server, and obtains an IPv6 address and other parameters from the server.

For details about the Relay-Forward and Relay-Reply messages, see DHCPv6 Packets in "DHCPv6 Configuration" in the *Huawei AR Series V200R010 Configuration Guide-IP Service*.

## 13.2.4 Option 18 and Option 37 Fields Supported by DHCPv6 Snooping

Functions of the Option 18 and Option 37 fields are similar to that of the Option 82 field. A device inserts the Option 18 and Option 37 fields into a DHCPv6 message to record the DHCPv6 client location.

NOTE

A device supports the Option 18 and Option 37 fields only after DHCPv6 snooping is enabled.

# 13.3 Application Scenarios for DHCP Snooping

 Copyright © Huawei Technologies Co., Ltd. 

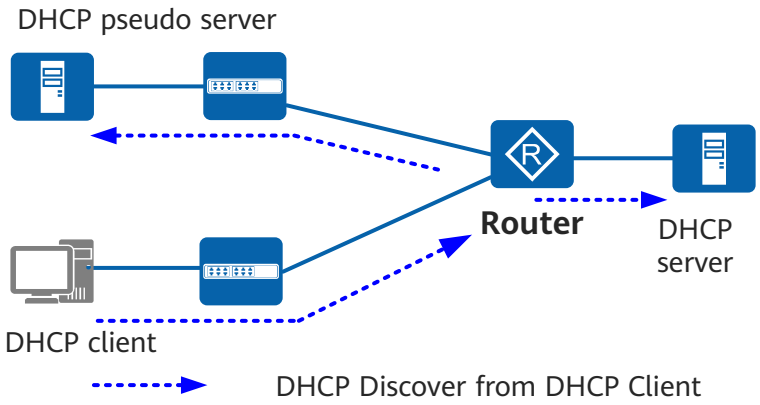
## 13.3.1 Defense Against Bogus DHCP Server Attacks

**Mechanism**

Because DHCP servers and DHCP clients lack authentication mechanisms between them, each DHCP server newly configured on a network assigns IP addresses and other network parameters to DHCP clients. If the assigned IP addresses and other network parameters are incorrect, errors may occur on the network.

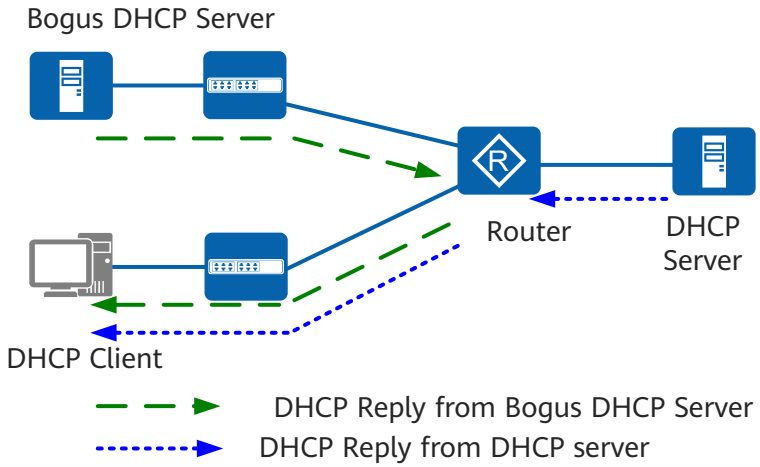
In **Figure 13-2**, authorized and unauthorized DHCP servers can receive DHCP Discover messages broadcast by DHCP clients.

**Figure 13-2** DHCP client sending DHCP Discover messages




If a bogus DHCP server sends a bogus DHCP Reply message with an incorrect gateway address, Domain Name System (DNS) server address, or IP address to a DHCP client, as shown in **Figure 13-3**, the DHCP client cannot obtain the correct IP address and required information. The authorized user then fails to access the network and user information security is compromised.

**Figure 13-3** Bogus DHCP server attack



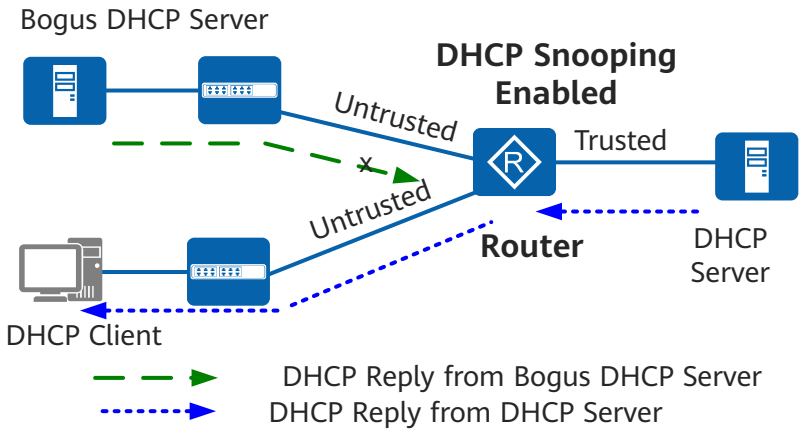

**Solution**

To prevent attacks from a bogus DHCP server, configure the trusted interface and untrusted interfaces on the device.


Copyright © Huawei Technologies Co., Ltd.

You can configure the interface directly or indirectly connected to the authorized DHCP server as the trusted interface and other interfaces as untrusted interfaces. The device then discards DHCP Reply messages received on untrusted interfaces, preventing bogus DHCP server attacks, as shown in **Figure 13-4**.

**Figure 13-4** Trusted interface and untrusted interfaces




## 13.3.2 Defense Against Bogus DHCP Message Attacks

**Mechanism**

An authorized DHCP client that has obtained an IP address sends a DHCP Request message or Release message to extend the lease time or to release the IP address. If an attacker continuously sends DHCP Request messages to the DHCP server to extend the lease time, the IP address cannot be reclaimed or obtained by authorized users. If an attacker sends forged DHCP Release messages to the DHCP server, the authorized user may be disconnected.

**Solution**

To prevent bogus DHCP message attacks, use the DHCP snooping binding table. The device checks DHCP Request messages and Release messages against binding entries to determine whether the messages are valid. Specifically, the device checks whether the VLAN IDs, IP addresses, MAC addresses, and interface IDs in DHCP messages match binding entries. If a message matches a binding entry, the device forwards the message. Otherwise, the device discards the message.

## 13.3.3 Defense Against DHCP Server DoS Attacks

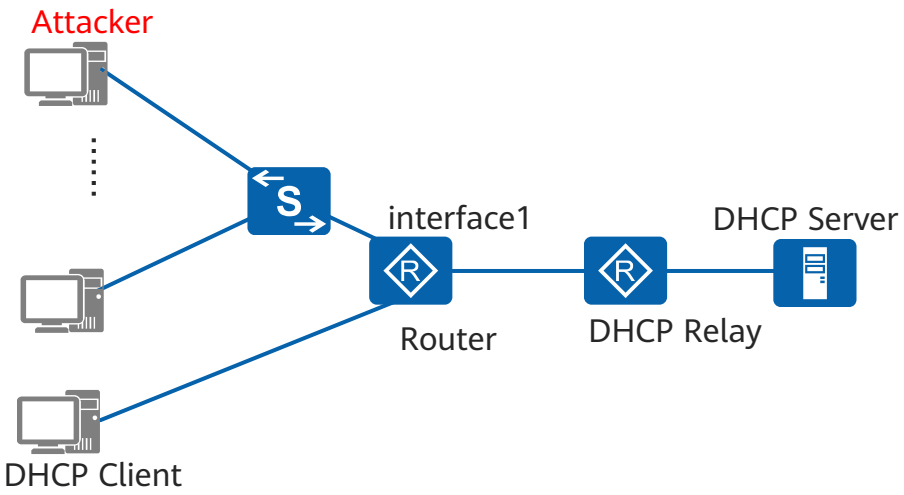
**Mechanism**

In **Figure 13-5**, if a large number of attackers request IP addresses on interface1, IP addresses in the IP address pool are exhausted. This results in no IP addresses being available for authorized users.

A DHCP server identifies the MAC address of a client based on the client hardware address (CHADDR) field in the DHCP Request message. If an attacker continuously applies for IP addresses by changing the value of the CHADDR field, IP addresses in the address pool on the DHCP server may be exhausted. As a result, authorized users cannot obtain IP addresses.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 13-5** Defense against DHCP server DoS attacks




**Solution**

To prevent DHCP server DoS attacks, enable DHCP snooping on the device and then set the maximum number of access DHCP clients allowed on the device or an interface. Only the allowed number of DHCP clients can obtain an IP address through the device or interface.

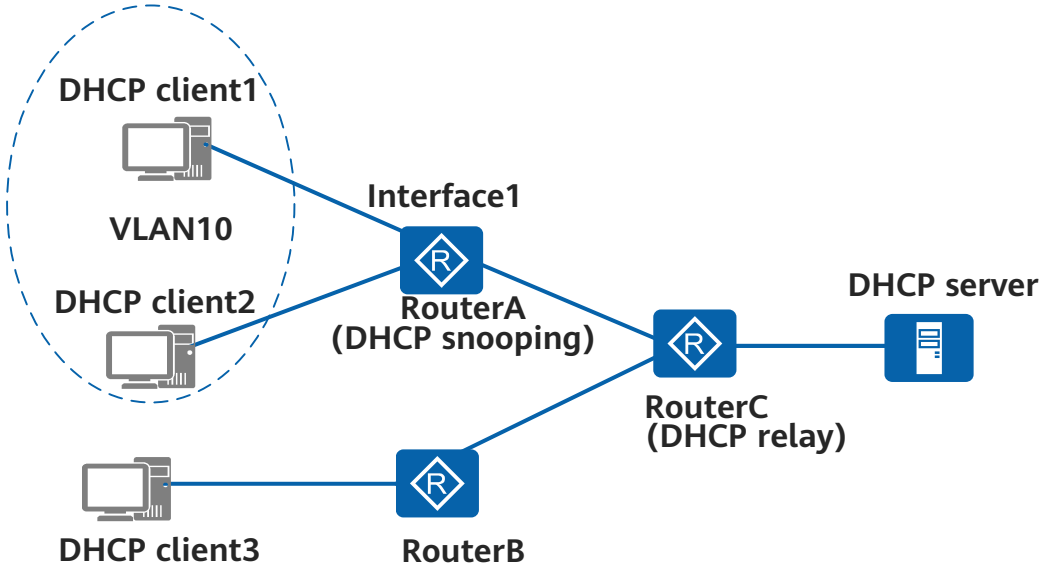
You can enable the device to check whether the MAC address in the Ethernet frame header matches the value of the CHADDR field in the DHCP message. If the two values match, the message is forwarded. Otherwise, the message is discarded.

## 13.3.4 Typical Application of the Option 82 Field

The DHCP Relay Agent Information Option (Option 82) field records the location of a DHCP client. A DHCP snooping-enabled device or a DHCP relay agent inserts the Option 82 field into a DHCP Request message to notify the DHCP server of the DHCP client location. Based on the Option 82 field, the DHCP server can properly assign an IP address and other configurations to the DHCP client, facilitating DHCP client security.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 13-6** Application of the Option 82 field




In **Figure 13-6**, clients use DHCP to obtain IP addresses. To improve network security, the administrator configures the device to control network access of clients connected to Interface1.

The DHCP server cannot detect the DHCP client location based only on the DHCP Request message. As a result, users in the same VLAN have the same rights to access network resources.

To address this issue, the administrator can enable the Option 82 insertion function after DHCP snooping is enabled on RouterA. Upon receiving a DHCP Request message, RouterA inserts the Option 82 field in the message to notify the DHCP server of the DHCP client location. The Option 82 field contains the MAC address, VLAN ID, and interface number of the client. The DHCP server can properly assign an IP address and other configurations to the client based on the IP address assignment or security policies on the server.

The Option 82 field records only the location of a DHCP client and is encapsulated in a DHCP Request message sent to the DHCP server. To deploy different IP address assignment or security policies for different clients, the DHCP server must support the Option 82 field and be configured with IP address assignment or security policies.

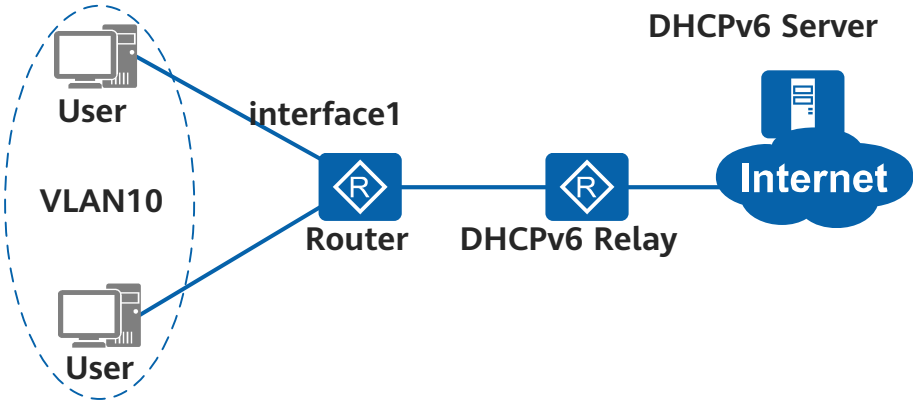
## 13.3.5 Detecting Client Locations Through an LDRA

An LDRA-enabled device can record client location information and forward the information to the DHCPv6 server. The DHCPv6 server then assigns IP addresses, accounting policies, and access control policies to the clients based on the client location information.

In **Figure 13-7**, users obtain IPv6 addresses through DHCPv6. The administrator wants to restrict the network access rights of the users on interface1 to improve network security.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 13-7** LDRA application




In the traditional process of allocating IPv6 addresses, the DHCPv6 server cannot obtain the physical locations of clients. Therefore, the server cannot assign specified IP addresses or policies to users on a certain interface.

To solve this issue, the administrator enables DHCP snooping and LDRA on the Router. The Router can then obtain the location information of clients and forward the information to the DHCPv6 server. The server assigns IP addresses and security policies to clients based on the client location information.

The LDRA function records only the client location information and forwards the information to the DHCPv6 server through Relay-Forward messages. The differentiated policies for IP address allocation, accounting, and access control are configured on the DHCPv6 server.

# 13.4 Licensing Requirements and Limitations for DHCP Snooping

## Involved Network Elements

Other network elements are not required.

## Licensing Requirements

DHCP snooping is a basic feature of a device and is not under license control.

## Feature Limitations

When deploying DHCP snooping on a device, pay attention to the following:

- The 4GE-2S, 4ES2GP-S, 4ES2G-S, and 9ES2 cards do not support DHCP snooping.
- AR100&AR120&AR150&AR160&AR200&AR1200 series do not support DHCPv6 snooping.
- DHCPv4 snooping can be configured on a Layer 2 access device and the first-hop DHCPv4 relay agent. DHCPv6 snooping can be configured on a Layer 2 access device and the first-hop DHCPv6 relay agent.
- The DHCP-triggered ARP learning function applies only to wired users and wireless users do not support this function.

 Copyright © Huawei Technologies Co., Ltd. 

# 13.5 Default Settings for DHCP Snooping

Table 13-1 lists the default settings for DHCP snooping.

**Table 13-1** Default settings for DHCP snooping

| Parameter | Default Setting |
| --- | --- |
| DHCP snooping globally and on an interface | Disabled |
| Interface status | Untrusted |
| Location transition for DHCP snooping users | Enabled |
| Association between DHCP snooping and ARP | Disabled |
| Option 82 | Disabled |
| Checking DHCP messages against the DHCP snooping binding table | Disabled |
| Checking whether the CHADDR field matches the source MAC address in the header of a DHCP Request message | Disabled |
| Checking whether the GIADDR field in a DHCP Request message is 0 | Disabled |

# 13.6 Configuring Basic Functions of DHCP Snooping

DHCP snooping allows DHCP clients to obtain IP addresses from authorized DHCP servers, and records mappings between IP addresses and MAC addresses of DHCP clients to a binding table.

## Pre-configuration Tasks

Before configuring DHCP snooping, configure the DHCP function. (For the DHCP configuration, see DHCP Configuration in the *Huawei AR Series V200R010 Configuration Guide - IP Service*.)

The procedures in **13.6.1 Enabling DHCP Snooping** and **13.6.2 Configuring an Interface as a Trusted Interface** also apply to DHCPv6 snooping.

## Configuration Procedure

Configure basic functions of DHCP snooping on a Layer 2 access device or the first DHCP relay agent from the device.


Copyright © Huawei Technologies Co., Ltd.

# 13.6.1 Enabling DHCP Snooping

## Context

DHCP snooping ensures security of the DHCP service. Before configuring DHCP snooping functions, you need to enable DHCP snooping.

You must enable DHCP snooping first in the system view, and then on an interface or in a VLAN.

NOTE

Use the **dhcp enable** command to enable DHCP globally before enabling DHCP snooping.

On the AR120&AR150&AR160&AR200 series and AR1200 series, before enabling DHCP snooping on an interface or in a VLAN, ensure that the DHCP relay or DHCP server function has been enabled on this interface or corresponding VLANIF interface; if they are not enabled, the device will not obtain the binding entries of users.

NOTE

DHCP snooping does not support the BOOTP protocol, which is used by diskless workstations. Therefore, DHCP snooping binding entries cannot be generated for diskless workstations. IPSG and DAI are implemented based on binding entries. For this reason, to use them on a diskless workstation, you must configure static binding entries by running the **user-bind static** command.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **dhcp snooping enable** [ **ipv4** | **ipv6** ]

DHCP snooping is globally enabled.

By default, DHCP snooping is globally disabled on the device.

NOTE

The **dhcp snooping enable** command in the system view is the prerequisite for DHCP snooping-related functions. After the **undo dhcp snooping enable** command is run, all DHCP snooping-related configurations of the device are deleted. After DHCP snooping is enabled again using the **dhcp snooping enable** command, all DHCP snooping-related configurations of the device are restored to the default configurations.

**Step 3** Enable DHCP snooping in the system, VLAN, or interface view.

- In the system view:

1. Run **dhcp snooping enable vlan** { *vlan-id1* [ **to** *vlan-id2* ] } &<1-10>

   DHCP snooping is enabled on the device.

   By default, DHCP snooping is disabled on the device.

- In the VLAN view or interface view:

1. Run **vlan** *vlan-id*

   The VLAN view is displayed.

 Copyright © Huawei Technologies Co., Ltd. 

Or run **interface** *interface-type interface-number*

The interface view is displayed.

2. Run **dhcp snooping enable**

DHCP snooping is enabled on the interface or in a VLAN.

By default, DHCP snooping is disabled on the device.

If you run this command in the VLAN view, the command takes effect on all the DHCP messages received by all interfaces from the specified VLAN. If you run this command in the interface view, the command takes effect on all the DHCP messages received by the specified interface.

If a single VLAN ID for 802.1Q encapsulation on a sub-interface is configured using the **dot1q termination vid** command, DHCP snooping cannot be enabled in the specified VLAN.

**----End**

## 13.6.2 Configuring an Interface as a Trusted Interface

### Context

To enable DHCP clients to obtain IP addresses only from authorized DHCP servers, configure the interfaces directly or indirectly connected to the DHCP servers trusted by the administrator as the trusted interfaces, and other interfaces as untrusted interfaces. This prevents bogus DHCP servers from assigning IP addresses to DHCP clients.

After enabling DHCP snooping on the interface or in the VLAN connected to the user, configure the interface connected to the DHCP server as the trusted interface, so that the dynamic DHCP snooping binding table is generated.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Configure the interface as the trusted interface in the interface view or VLAN view.

If you run this command in the VLAN view, the command takes effect only on DHCP messages in this VLAN received from interfaces that belong to this VLAN. If you run the **dhcp snooping trusted** command in the interface view, the command takes effect for all the DHCP messages received on the specified interface.

- In the interface view:

1. Run **interface** *interface-type interface-number*

The interface view is displayed.

2. Run **dhcp snooping trusted**

The interface is configured as the trusted interface.

By default, an interface is an untrusted interface.

 Copyright © Huawei Technologies Co., Ltd. 

- In the VLAN view:

1. Run **vlan** *vlan-id*

   The VLAN view is displayed.

2. Run **dhcp snooping trusted interface** *interface-type interface-number*

   The interface is configured as the trusted interface.

   By default, an interface is an untrusted interface.

**----End**

# 13.6.3 (Optional) Enabling Location Transition for DHCP Snooping Users

## Context

In mobile applications, if a user goes online from interfaceA and then switches to interfaceB, you need to enable location transition for DHCP snooping users.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **dhcp snooping user-transfer enable**

Location transition is enabled for DHCP snooping users.

By default, location transition is enabled for DHCP snooping users.

**----End**

# 13.6.4 (Optional) Configuring Association Between ARP and DHCP Snooping

## Context

When a DHCP snooping-enabled device receives a DHCP Release message sent from a DHCP client, the device deletes the binding entry of the DHCP client. However, if a client is unexpectedly disconnected and cannot send a DHCP Release message, the device cannot immediately delete the binding entry of the DHCP client.

After association between ARP and DHCP snooping is enabled, the DHCP snooping-enabled device performs an ARP probe to detect the IP address when the ARP entry mapping an IP address ages. If the DHCP client is not detected after a specified number of probes, the device deletes the ARP entry. The device then performs an ARP probe again to detect the IP address. If the DHCP client still cannot be detected after a specified number of probes, the device deletes the binding entry of the DHCP client.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

A device supports association between ARP and DHCP snooping only when the device functions as a DHCP relay agent.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **arp dhcp-snooping-detect enable**

Association between ARP and DHCP snooping is enabled.

By default, association between ARP and DHCP snooping is disabled.

**----End**

# 13.6.5 (Optional) Configuring the Device to Discard DHCP Request Messages When GIADDR Field Is Not 0

## Context

The gateway IP address (GIADDR) field in a DHCP Request message records the IP address of the first DHCP relay agent through which the DHCP Request message passes. When a DHCP client sends a DHCP Request message, if the DHCP server and client are on different network segments, the first DHCP relay agent fills its own IP address in the GIADDR field before forwarding the DHCP Request message. The DHCP server then uses the IP address in this field to locate the DHCP client and select an appropriate address pool from which to assign an IP address to the client.

To ensure that the device obtains parameters such as MAC addresses for generating a binding table, enable DHCP snooping on Layer 2 access devices or the first DHCP relay agent. This ensures that the GIADDR field in the DHCP Request messages received by the DHCP snooping-enabled device is 0. If the GIADDR field is not 0, the message is considered to be invalid and discarded.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Enable the device to check whether the GIADDR field in the DHCP Request message is 0 in the VLAN view or interface view.

1. Run **vlan** *vlan-id*

   The VLAN view is displayed.

   Or run **interface** *interface-type interface-number*

   The interface view is displayed.
2. Run **dhcp snooping check dhcp-giaddr enable**

 Copyright © Huawei Technologies Co., Ltd. 

The device is enabled to check whether the GIADDR field in a DHCP Request message is 0.

By default, the device does not check whether the GIADDR field in a DHCP Request message is 0.

If you run this command in the VLAN view, the command takes effect on all the DHCP messages in the specified VLAN received by all the interfaces on the device. If you run this command in the interface view, the command takes effect on all the DHCP messages received by the specified interface.

**----End**

# 13.6.6 (Optional) Disabling DHCP Snooping on an Interface

## Context

When DHCP snooping is enabled in a VLAN, all interfaces in this VLAN will have DHCP snooping enabled. To disable DHCP snooping on a specified interface, run the **dhcp snooping disable** command on this interface. After DHCP snooping is disabled on an interface, users on this interface can go online, but dynamic DHCP binding entries are not generated for the users.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface** *interface-type interface-number*

The interface view is displayed.

**Step 3** Run **dhcp snooping disable**

DHCP snooping is disabled on an interface.

By default, if the **dhcp snooping enable** command is run on an interface or in the VLAN to which an interface belongs, DHCP snooping is enabled on this interface.

**----End**

# 13.6.7 Verifying the DHCP Snooping Configuration

## Context

You can verify the DHCP snooping configuration after the configuration is complete.

## Procedure

- Run the **display dhcp snooping** [ **interface** *interface-type interface-number* | **vlan** *vlan-id* ] command to view DHCP snooping running information.
- Run the **display dhcp snooping configuration** [ **vlan** *vlan-id* | **interface** *interface-type interface-number* ] command to view the DHCP snooping configuration.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **display dhcp snooping user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [ **verbose** ] command to check the DHCP snooping binding table.
- Run the **display dhcpv6 snooping user-bind** { { **interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **vlan** *vlan-id* }* | **all** } [ **verbose** ] command to check the DHCPv6 snooping binding table.
- Run the **display dhcp snooping statistics** command to check statistics on the received DHCP messages.

**----End**

# 13.7 Configuring DHCP Snooping Attack Mitigation

After basic DHCP snooping functions are configured, DHCP clients can obtain IP addresses from the authorized DHCP server, preventing attacks on the network from bogus DHCP servers. However, many other DHCP attacks exist on the network. To mitigate these attacks, configure DHCP snooping attack mitigation functions on the device as required.

In this chapter, the function in **Configuring Defense Against Bogus DHCP Message Attacks** and the function in step 2 of **Configuring Defense Against DHCP Server DoS Attacks** are also applicable to DHCPv6 snooping.

## Prerequisites

Basic DHCP snooping functions have been configured.

## 13.7.1 Configuring Defense Against Bogus DHCP Server Attacks

### Context

After DHCP snooping is enabled and a trusted interface is configured, the device ensures DHCP clients obtain IP addresses from the authorized DHCP server, preventing attacks from bogus DHCP servers. However, the location of the bogus DHCP server cannot be detected, meaning the network security is still at risk.

After DHCP server detection is enabled, the DHCP snooping-enabled device checks information about the DHCP server, such as its IP address and connecting port number, in the DHCP Reply messages and records the information in the log. You can refer to these logs to check whether bogus DHCP servers exist on the network.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **dhcp server detect**

DHCP server detection is enabled.

 Copyright © Huawei Technologies Co., Ltd. 

By default, detection of DHCP servers is disabled.

**----End**

## 13.7.2 Configuring Defense Against Bogus DHCP Message Attacks

### Context

If an attack pretends to be an authorized user to send a bogus DHCP message to the DHCP server on a DHCP network, the authorized user cannot use the IP address or goes offline unexpectedly. After the DHCP snooping binding table is generated, the device can check DHCP messages against the binding table. Only messages that match the binding table can be forwarded; otherwise, the messages are discarded. This prevents unauthorized users from sending bogus DHCP messages to renew or release IP addresses.

### Procedure

**Step 1** Enable a device to check DHCP messages against the DHCP snooping binding table.

If the function is configured in the VLAN view, it takes effect on all the interfaces in the VLAN; if the function is configured in the interface view, it takes effect only on the interface.

1. Run **system-view**

   The system view is displayed.
2. Run **vlan** *vlan-id* or **interface** *interface-type interface-number*

   The VLAN or interface view is displayed, respectively.
3. Run **dhcp snooping check user-bind enable**

   The device is enabled to check DHCP messages against the DHCP snooping binding table.

   By default, a device is not enabled to check DHCP messages against the DHCP snooping binding table.
4. Run **dhcp snooping check mac-address enable**

   The function of checking whether the CHADDR field is the same as the source MAC address of the header of a DHCP Request message is enabled.

   By default, the function of checking whether the CHADDR field is the same as the source MAC address of the header of a DHCP Request message is disabled.

**Step 2** (Optional) Enable the DHCP snooping alarm function.

1. Run **system-view**

   The system view is displayed.
2. Run **interface** *interface-type interface-number*

   The interface view is displayed.

 Copyright © Huawei Technologies Co., Ltd. 

3. Run **dhcp snooping alarm** { **user-bind** | **mac-address** | **untrust-reply** } **enable**

   The DHCP snooping alarm function is enabled.

   By default, the DHCP snooping alarm function is disabled.

**Step 3** (Optional) Configure the alarm threshold.

The alarm threshold can be set both in the system view and interface view. If the alarm threshold is configured in the system view and interface view, the smaller value takes effect.

- In the system view:

1. Run **system-view**

   The system view is displayed.
2. Run **dhcp snooping alarm threshold** *threshold*

   The alarm threshold for the number of DHCP snooping-discarded messages is configured.

   If this command is run in the system view, it takes effect on all the interfaces of the device.

   By default, the alarm threshold for the number of DHCP snooping-discarded messages is 100.

- In the interface view:

1. Run **system-view**

   The system view is displayed.
2. Run **interface** *interface-type interface-number*

   The interface view is displayed.
3. Run **dhcp snooping alarm** { **user-bind** | **mac-address** | **untrust-reply** } **threshold** *threshold*

   The alarm threshold for the number of DHCP snooping-discarded messages is configured.

   By default, the global alarm threshold for the number of DHCP snooping-discarded messages is 100, and the alarm threshold for the number of DHCP snooping-discarded messages on an interface is the value configured using the **dhcp snooping alarm threshold** command in the system view.

**----End**

## 13.7.3 Configuring Defense Against DHCP Server DoS Attacks

### Context

If attackers maliciously apply for IP addresses from the DHCP server, the IP address pool becomes exhausted, preventing authorized users from obtaining IP addresses. This can happen if attackers continuously apply for IP addresses by changing the client hardware address (CHADDR) field, which is the field that DHCP servers generally use to identify the MAC address of a DHCP client.

 Copyright © Huawei Technologies Co., Ltd. 

To prevent DHCP users on some interfaces from maliciously applying for IP addresses, you can limit the number of DHCP snooping binding entries that can be learned by an interface. When the number of DHCP snooping binding entries reaches the maximum value, no DHCP client can obtain an IP address through the interface. To prevent attacks carried out by continuously changing the CHADDR field in the DHCP Request message, enable the device to check whether the MAC address in the Ethernet frame header matches the CHADDR field in the DHCP message. With this function enabled, the message is only forwarded if the two values match.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Set the maximum number of DHCP snooping binding entries to be learned by an interface in the VLAN, or interface view.

1. Run **vlan** *vlan-id*

   The VLAN view is displayed.

   Or run **interface** *interface-type interface-number*

   The interface view is displayed.
2. Run **dhcp snooping max-user-number** *max-user-number*

   The maximum number of DHCP snooping binding entries is set on the interface.

   If you run this command in the VLAN view, the command takes effect for all the interfaces in the VLAN.

**Step 3** Enable the device to check the CHADDR field in the message in the VLAN view or interface view.

1. Run **vlan** *vlan-id*

   The VLAN view is displayed.

   Or run **interface** *interface-type interface-number*

   The interface view is displayed.
2. Run **dhcp snooping check mac-address enable**

   The device is enabled to check whether the MAC address in the Ethernet frame header matches the CHADDR field in the DHCP message.

   By default, the device does not check whether the MAC address in the Ethernet frame header matches the CHADDR field in the DHCP message.

   If you run the **dhcp snooping check mac-address enable** command in the VLAN view, the command takes effect on all the DHCP messages in the specified VLAN received by all the interfaces on the device. If you run the **dhcp snooping check mac-address enable** command in the interface view, the command takes effect for all the DHCP messages received on the interface.

 Copyright © Huawei Technologies Co., Ltd. 

3. Run **quit**

   Return to the system view.

**Step 4** (Optional) Set the alarm threshold for the number of messages discarded by DHCP snooping in the system view or interface view.

- In the system view:

1. Run **dhcp snooping alarm threshold** *threshold*

   The global alarm threshold for the number of discarded messages by DHCP snooping is set.

   If you run this command in the system view, the command takes effect for all the interfaces on the device.

   By default, the global alarm threshold for the number of messages discarded by DHCP snooping is 100.

- In the interface view:

1. Run **interface** *interface-type interface-number*

   The interface view is displayed.

2. Run **dhcp snooping alarm mac-address threshold** *threshold*

   The alarm threshold for the number of DHCP messages discarded because the CHADDR field in the DHCP messages does not match the source MAC address in the Ethernet frame header is set.

   By default, an alarm is generated in the system when at least 100 DHCP snooping messages are discarded, and the alarm threshold on an interface is set using the **dhcp snooping alarm threshold** command in the system view.

   NOTE

   If the alarm threshold is set in the system view and interface view, the smaller value takes effect.

**----End**

# 13.7.4 Verifying the DHCP Snooping Attack Defense Configuration

## Context

After DHCP snooping attack defense is completely configured, check the configured parameters.

## Procedure

- Run the **display dhcp snooping** [ **interface** *interface-type interface-number* | **vlan** *vlan-id* ] command to view DHCP snooping running information.
- Run the **display dhcp snooping configuration** [ **vlan** *vlan-id* | **interface** *interface-type interface-number* ] command to view the DHCP snooping configuration.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **display dhcp snooping statistics** command to check statistics on the received DHCP messages.

**----End**

# 13.8 Inserting the Option 82 Field in a DHCP Message

## Context

The Option 82 field records the location of a DHCP client, and is inserted into a DHCP Request message before being sent to the DHCP server. This allows the DHCP server to assign an IP address and other configurations to the DHCP client, facilitating DHCP client security.

NOTE

- DHCP Option 82 must be configured on the user side of a device; otherwise, the DHCP message sent to the DHCP server will not carry Option 82.
- The total length of all Option82 fields must be between 1 byte to 255 bytes. If their total length exceeds 255 bytes, some Option82 information will be lost.
- There is no limit on the number of Option 82 fields configured on a device. However, a large number of Option 82 fields will occupy a lot of memory and slow down device processing. To ensure device performance, take into account the service requirements and device memory size when configuring Option 82 fields.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** You can configure the device to insert the Option 82 field in a DHCP message in the interface view or VLAN view.

| View | Steps |
| --- | --- |
| VLAN view | 1. Run the **vlan** *vlan-id* command to enter the VLAN view.<br>2. Run the **dhcp option82** { **insert** \| **rebuild** } **enable** command to enable the device to insert the Option 82 field in a DHCP message.<br>By default, the device is disabled from inserting the Option 82 field in a DHCP message.<br>3. Run the **quit** command to return to the system view. |
| Interface view | 1. Run the **interface** *interface-type interface-number* command to enter the interface view.<br>2. Run the **dhcp option82** { **insert** \| **rebuild** } **enable** command to enable the device to insert the Option 82 field in a DHCP message.<br>By default, the device is disabled from inserting the Option 82 field in a DHCP message.<br>3. Run the **quit** command to return to the system view. |

 Copyright © Huawei Technologies Co., Ltd. 

**Step 3** (Optional) You can configure the format of the Option 82 field in the system or interface view. If the configuration is performed in the system view, the configuration takes effect for all interfaces on the device. If the configuration is performed in the interface view, the configuration takes effect only for the specified interface.

| View | Steps |
| --- | --- |
| System view | 1. Run the **dhcp option82** [ **vlan** *vlan-id* ] [ **ce-vlan** *ce-vlan-id* ] [ **circuit-id** \| **remote-id** ] **format** { **default** \| **common** \| **extend** \| **user-defined** *text* } command to configure the format of the Option 82 field in a DHCP message.<br>By default, the format of the Option 82 field in a DHCP message is **default**. |
| Interface view | 1. Run the **interface** *interface-type interface-number* command to enter the interface view.<br>2. Run the **dhcp option82** [ **vlan** *vlan-id* ] [ **ce-vlan** *ce-vlan-id* ] [ **circuit-id** \| **remote-id** ] **format** { **default** \| **common** \| **extend** \| **user-defined** *text* } command to configure the format of the Option 82 field in a DHCP message.<br>By default, the format of the Option 82 field in a DHCP message is **default**.<br>3. Run the **quit** command to return to the system view. |

**Step 4** (Optional) Run **dhcp option82 subscriber-id format** { **ascii** *ascii-text* | **hex** *hex-text* }

The Sub6 suboption is inserted into the Option 82 field of DHCP messages and the format of the Sub6 suboption is configured.

By default, the Sub6 suboption is not inserted into the Option 82 field of DHCP messages.

**Step 5** (Optional) Configure suboptions inserted into the DHCP Option 82 field in the system view, VLAN view, or interface view. If the configuration is performed in the system view, the configuration takes effect for all interfaces on the device. If the configuration is performed in the VLAN view, the configuration takes effect for all DHCP messages from this VLAN that are received by all interfaces. If the configuration is performed in the interface view, the configuration takes effect only for the specified interface.

| View | Steps |
| --- | --- |
| System view | 1. Run the **dhcp option82 encapsulation** { **circuit-id** \| **remote-id** \| **subscriber-id** } * command to configure suboptions inserted into the DHCP Option 82 field.<br>By default, the circuit-id (CID) and remote-id (RID) suboptions are inserted into the DHCP Option 82 field. |

 Copyright © Huawei Technologies Co., Ltd. 

| View | Steps |
| --- | --- |
| VLAN view | 1. Run the **vlan** *vlan-id* command to enter the VLAN view.<br>2. Run the **dhcp option82 encapsulation** { **circuit-id** \| **remote-id** \| **subscriber-id** } * command to configure suboptions inserted into the DHCP Option 82 field. By default, the circuit-id (CID) and remote-id (RID) suboptions are inserted into the DHCP Option 82 field.<br>3. Run the **quit** command to return to the system view. |
| Interface view | 1. Run the **interface** *interface-type interface-number* command to enter the interface view.<br>2. Run the **dhcp option82 encapsulation** { **circuit-id** \| **remote-id** \| **subscriber-id** } * command to configure suboptions inserted into the DHCP Option 82 field. By default, the circuit-id (CID) and remote-id (RID) suboptions are inserted into the DHCP Option 82 field.<br>3. Run the **quit** command to return to the system view. |

**----End**

## Verifying the Configuration

- Run the **display dhcp option82 configuration** [ **vlan** *vlan-id* | **interface** *interface-type interface-number* ] command to view the DHCP Option 82 configuration.

# 13.9 Configuring the LDRA to Detect Client Locations

## Context

To allow a DHCPv6 server to detect client locations on a DHCPv6 network, configure the lightweight DHCPv6 relay agent (LDRA) on the client-side access device.

After the LDRA is configured on a DHCPv6 network with a large number of trusted clients, disable the device from generating DHCP snooping binding entries. Without this function enabled, new users cannot go online if the number of DHCP snooping binding entries reaches the upper limit. In addition, the LDRA-enabled device inserts the interface-ID or remote-ID option into the Relay-Forward message to record client location information. Configure the formats of interface-ID and remote-ID depending on the actual location of users on the network.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **vlan** *vlan-id*

 Copyright © Huawei Technologies Co., Ltd. 

The VLAN view is displayed.

**Step 3** Run **dhcpv6 snooping relay-information enable** [ **trust** ]

The LDRA is enabled for DHCPv6 snooping.

By default, the LDRA is disabled for DHCPv6 snooping.

**Step 4** Run **quit**

Return to the system view.

**Step 5** (Optional) Run **dhcpv6 interface-id format** { **default** | **user-defined** *text* }

The format of the interface-id option in the DHCPv6 packets is configured.

By default, the interface-id option is in the **default** format.

**Step 6** (Optional) Run **dhcpv6 remote-id format** { **default** | **user-defined** *text* }

The format of the remote-id option in the DHCPv6 packets is configured.

By default, the remote-id option is in the **default** format.

**Step 7** (Optional) Disable the interface from generating DHCP snooping binding entries after the DHCP snooping function has been enabled.

When this configuration is performed in the VLAN view, the configuration takes effect for all DHCP users belonging to this VLAN on all interfaces. When this configuration is performed in the interface view, the configuration takes effect for all DHCP users connecting to this interface.

By default, an interface generates DHCP snooping binding entries after DHCP snooping is enabled.

| Configuration Dimension | Step |
| --- | --- |
| VLAN-based configuration | For a batch of VLANs in the system view<br>• Run the **dhcp snooping enable no-user-binding vlan** { *vlan-id1* [ **to** *vlan-id2* ] }&<1-10> command to disable the interfaces from generating DHCP snooping binding entries after DHCP snooping is enabled.<br>For a single VLAN in the VLAN view<br>1. Run the **vlan** *vlan-id* command to enter the VLAN view.<br>2. Run the **dhcp snooping enable no-user-binding** command to disable the interfaces from generating DHCP snooping binding entries after DHCP snooping is enabled.<br>3. Run the **quit** command to return to the system view. |
| Interface-based configuration | 1. Run the **interface** *interface-type interface-number* command to enter the interface view.<br>2. Run the **dhcp snooping enable no-user-binding** command to disable the interfaces from generating DHCP snooping binding entries after DHCP snooping is enabled.<br>3. Run the **quit** command to return to the system view. |

 Copyright © Huawei Technologies Co., Ltd. 

**----End**

# 13.10 Inserting the Option 18 or Option 37 Field in a DHCPv6 Message

## Context

The function of inserting the Option 18 or Option 37 field in a DHCPv6 message is similar to that of inserting the Option 82 field in a DHCPv4 message. The Option 18 field contains the interface ID of a client and the Option 37 field contains the MAC address of a client. A device inserts the Option 18 or Option 37 field to a DHCPv6 Request message to notify the DHCP server of the DHCPv6 client location. This allows the DHCP server to assign an IP address and other configurations to the DHCPv6 client, facilitating DHCP client security.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface** *interface-type interface-number*

The interface view is displayed.

**Step 3** Run **dhcpv6** { **option18** | **option37** } { **insert** | **rebuild** } **enable**

The device is enabled to insert the Option 18 or Option 37 field to a DHCPv6 Request message.

By default, the device is disabled from inserting the Option 18 or Option 37 field in a DHCPv6 message.

**NOTE**

If you run the **dhcpv6 { option18 | option37 } enable** command in the VLAN view, the command takes effect for all the DHCPv6 messages received from the specified VLAN. If you run the **dhcpv6 { option18 | option37 } enable** command in the interface view, the command takes effect for all the DHCPv6 messages received on the specified interface.

**Step 4** Run **quit**

Return to the system view.

**Step 5** (Optional) You can configure the format of Option 18 field inserted in DHCPv6 messages in the system view, VLAN view, or interface view.

- In the system view:
  a. Run **dhcpv6 option18** [ **vlan** *vlan-id* ] [ **ce-vlan** *ce-vlan-id* ] **format user-defined** *text*

     The format of Option 18 field inserted in DHCPv6 messages is configured.

     By default, the format of Option 18 field inserted in DHCPv6 messages is not configured.

 Copyright © Huawei Technologies Co., Ltd. 

- In the VLAN view:
  a. Run **vlan** *vlan-id*

     The VLAN view is displayed.
  b. Run **dhcpv6 option18 format user-defined** *text*

     The format of Option 18 field inserted in DHCPv6 messages is configured.

     By default, the format of Option 18 field inserted in DHCPv6 messages is not configured.
- In the interface view:
  a. Run **interface** *interface-type interface-number*

     The interface view is displayed.
  b. Run **dhcpv6 option18** [ **vlan** *vlan-id* ] [ **ce-vlan** *ce-vlan-id* ] **format user-defined** *text*

     The format of Option 18 field inserted in DHCPv6 messages is configured.

     By default, the format of Option 18 field inserted in DHCPv6 messages is not configured.

NOTE

If you run the **dhcpv6 option18 format** command in the system view, the command takes effect for the Option 18 field in all DHCPv6 messages. If you run the **dhcpv6 option18 format** command in the VLAN view, the command takes effect for the Option 18 field in all DHCPv6 messages received from the specified VLAN. If you run the **dhcpv6 option18 format** command in the interface view, the command takes effect for the Option 18 field in all DHCPv6 messages received on the specified interface.

**Step 6** (Optional) Configure the format of Option 37 field inserted in DHCPv6 messages in the system view, VLAN view, or interface view.

- In the system view:
  a. Run **dhcpv6 option37** [ **vlan** *vlan-id* ] [ **ce-vlan** *ce-vlan-id* ] **format user-defined** *text*

     The format of Option 37 field inserted in DHCPv6 messages is configured.

     By default, the format of Option 37 field inserted in DHCPv6 messages is not configured.
- In the VLAN view:
  a. Run **vlan** *vlan-id*

     The VLAN view is displayed.
  b. Run **dhcpv6 option37 format user-defined** *text*

     The format of Option 37 field inserted in DHCPv6 messages is configured.

     By default, the format of Option 37 field inserted in DHCPv6 messages is not configured.
- In the interface view:
  a. Run **interface** *interface-type interface-number*

     The interface view is displayed.
  b. Run **dhcpv6 option37** [ **vlan** *vlan-id* ] [ **ce-vlan** *ce-vlan-id* ] **format user-defined** *text*

     The format of Option 37 field inserted in DHCPv6 messages is configured.

 Copyright © Huawei Technologies Co., Ltd. 

By default, the format of Option 37 field inserted in DHCPv6 messages is not configured.

NOTE

If you run the **dhcpv6 option37 format** command in the system view, the command takes effect for the Option 37 field in all DHCPv6 messages. If you run the **dhcpv6 option37 format** command in the VLAN view, the command takes effect for the Option 37 field in all DHCPv6 messages received from the specified VLAN. If you run the **dhcpv6 option37 format** command in the interface view, the command takes effect for the Option 37 field in all DHCPv6 messages received on the specified interface.

**----End**

# 13.11 Maintaining DHCP Snooping

## 13.11.1 Clearing DHCP Snooping Statistics

### Context

NOTICE

The cleared statistics cannot be restored. Exercise caution when you run the commands.

### Procedure

- Run the **reset dhcp snooping statistics global** command in the user view to clear statistics on globally discarded DHCP messages.
- Run the **reset dhcp snooping statistics interface** *interface-type interface-number* [ **vlan** *vlan-id* ] command in the user view to clear statistics on discarded DHCP messages on an interface.
- Run the **reset dhcp snooping statistics vlan** *vlan-id* [ **interface** *interface-type interface-number* ] command in the user view to clear statistics on discarded DHCP messages in a VLAN.

**----End**

## 13.11.2 Clearing DHCP Snooping Binding Entries

### Context

After the networking environment changes, DHCP snooping binding entries do not age immediately. The following information in DHCP snooping binding entries may change, causing packet forwarding failure:

- VLAN to which a DHCP client belongs.
- Interface to which DHCP clients are connected.

Before changing the networking environment, clear all DHCP snooping binding entries manually so that the device generates a new DHCP snooping binding table based on the new networking environment.

 Copyright © Huawei Technologies Co., Ltd. 

NOTICE

After the DHCP snooping binding entries are cleared, network communication can be recovered only after all the DHCP users connected to the device re-log in and new binding entries are generated. Exercise caution when you run the command.

### Procedure

- Run the **reset dhcp snooping user-bind** [ [ **vlan** *vlan-id* | **interface** *interface-type interface-number* ] * | **ip-address** [ *ip-address* ] | **ipv6-address** [ *ipv6-address* ] ] command in the user view to clear DHCP snooping binding entries.

**----End**

## 13.11.3 Backing Up DHCP Snooping Binding Entries

### Context

If binding entries are not backed up, the binding entries will be lost after the device restarts. DHCP users must log in again so that the device can generate DHCP snooping binding entries for DHCP users to communicate. After DHCP snooping binding entries are backed up, DHCP snooping binding entries can be restored after the device restarts.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **dhcp snooping user-bind autosave** *file-name* [ **write-delay** *delay-time* ]

The device is enabled to back up dynamic DHCP snooping binding entries.

By default, local automatic backup of the DHCP snooping binding table is disabled.

**----End**

# 13.12 Configuration Examples for DHCP Snooping

## 13.12.1 Example for Configuring DHCP Snooping Attack Defense

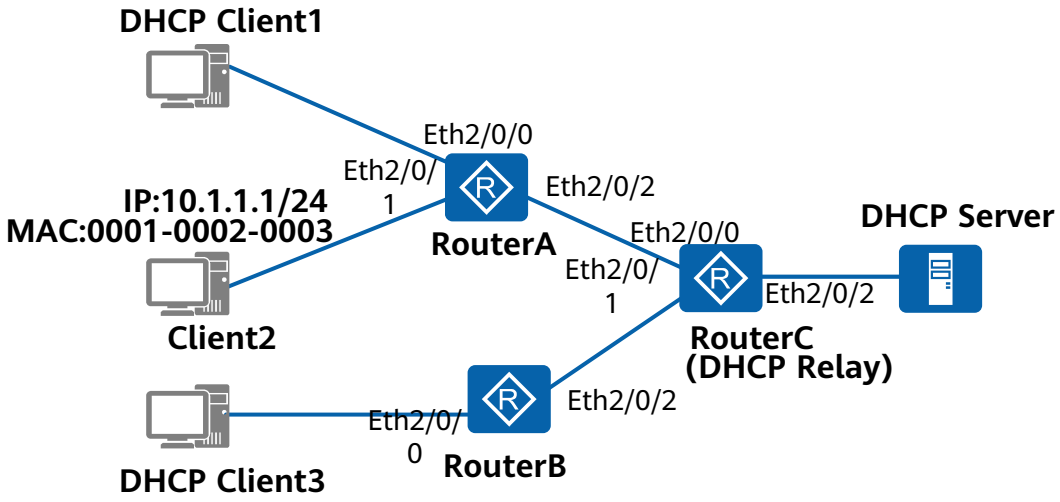
### Networking Requirements

In **Figure 13-8**, RouterA and RouterB are access devices, and RouterC is a DHCP relay agent. Client1 and Client2 are connected to RouterA through Eth2/0/0 and Eth2/0/1 respectively. Client3 is connected to RouterB through Eth2/0/0. Client1 and Client3 obtain IP addresses using DHCP, while Client2 uses the static IP address. Attacks from unauthorized users prevent authorized users from obtaining

 Copyright © Huawei Technologies Co., Ltd. 

IP addresses. The administrator needs to enable the device to defend against DHCP attacks on the network and provide better service to DHCP clients.

**Figure 13-8** Networking diagram for configuring DHCP snooping attack defense




## Configuration Roadmap

The configuration roadmap is as follows:

1. Enable DHCP snooping.
2. Configure an interface as the trusted interface to ensure that DHCP clients obtain IP addresses from the authorized server.
3. Enable association between ARP and DHCP snooping to enable the device to update the binding entries when a DHCP user is disconnected.
4. Enable the device to check DHCP messages against the binding table to prevent bogus DHCP message attacks.
5. Set the maximum number of access DHCP clients and enable the device to check whether the MAC address in the Ethernet frame header matches the CHADDR field in the DHCP message to prevent DHCP server DoS attacks.
6. Configure the trap function for the number of discarded messages and the rate limit.

## Procedure

**Step 1** Enable DHCP snooping.

# Enable DHCP snooping globally.

```
<Huawei> system-view
[Huawei] sysname RouterC
[RouterC] dhcp enable
[RouterC] dhcp snooping enable
```

# Enable DHCP snooping on the user-side interface. Eth2/0/0 is used as an example. The configuration on Eth2/0/1 is the same as the configuration on Eth2/0/0 and is not mentioned here.

 Copyright © Huawei Technologies Co., Ltd. 

```
[RouterC] interface ethernet 2/0/0
[RouterC-Ethernet2/0/0] dhcp snooping enable
[RouterC-Ethernet2/0/0] quit
```

**Step 2** Configure the interface connected to the DHCP server as the trusted interface.

```
[RouterC] interface ethernet 2/0/2
[RouterC-Ethernet2/0/2] dhcp snooping trusted
[RouterC-Ethernet2/0/2] quit
```

**Step 3** Enable association between ARP and DHCP snooping.

```
[RouterC] arp dhcp-snooping-detect enable
```

**Step 4** Enable the device to check DHCP messages against the DHCP snooping binding table.

# Configure the user-side interface. Eth2/0/0 is used as an example. The configuration on Eth2/0/1 is the same as the configuration on Eth2/0/0 and is not mentioned here.

```
[RouterC] interface ethernet 2/0/0
[RouterC-Ethernet2/0/0] dhcp snooping check user-bind enable
[RouterC-Ethernet2/0/0] quit
```

**Step 5** Enable the device to check whether the GIADDR field in a DHCP Request message is 0.

# Configure the user-side interface. Eth2/0/0 is used as an example. The configuration on Eth2/0/1 is the same as the configuration on Eth2/0/0 and is not mentioned here.

```
[RouterC] interface ethernet 2/0/0
[RouterC-Ethernet2/0/0] dhcp snooping check dhcp-giaddr enable
[RouterC-Ethernet2/0/0] quit
```

**Step 6** Set the maximum number of access users allowed on the interface and enable the device to check the CHADDR field.

# Configure the user-side interface. Eth2/0/0 is used as an example. The configuration on Eth2/0/1 is the same as the configuration on Eth2/0/0 and is not mentioned here.

```
[RouterC] interface ethernet 2/0/0
[RouterC-Ethernet2/0/0] dhcp snooping max-user-number 20
[RouterC-Ethernet2/0/0] dhcp snooping check mac-address enable
[RouterC-Ethernet2/0/0] quit
```

**Step 7** Configure the trap function for the number of discarded messages and the rate limit.

# Enable the trap function for discarding messages and set the alarm threshold. Eth2/0/0 is used as an example. The configuration on Eth2/0/1 is the same as the configuration on Eth2/0/0 and is not mentioned here.

```
[RouterC] interface ethernet 2/0/0
[RouterC-Ethernet2/0/0] dhcp snooping alarm mac-address enable
[RouterC-Ethernet2/0/0] dhcp snooping alarm user-bind enable
[RouterC-Ethernet2/0/0] dhcp snooping alarm untrust-reply enable
[RouterC-Ethernet2/0/0] dhcp snooping alarm mac-address threshold 120
[RouterC-Ethernet2/0/0] dhcp snooping alarm user-bind threshold 120
[RouterC-Ethernet2/0/0] dhcp snooping alarm untrust-reply threshold 120
[RouterC-Ethernet2/0/0] quit
```

**Step 8** Verify the configuration.

 Copyright © Huawei Technologies Co., Ltd. 

# Run the **display dhcp snooping configuration** command to view the DHCP snooping configuration.

```
[RouterC] display dhcp snooping configuration
#
dhcp snooping enable
arp dhcp-snooping-detect enable
#
interface Ethernet2/0/0
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check user-bind enable
 dhcp snooping alarm user-bind enable
 dhcp snooping alarm user-bind threshold 120
 dhcp snooping check mac-address enable
 dhcp snooping alarm mac-address enable
 dhcp snooping alarm mac-address threshold 120
 dhcp snooping alarm untrust-reply enable
 dhcp snooping alarm untrust-reply threshold 120
 dhcp snooping max-user-number 20
#
interface Ethernet2/0/1
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check user-bind enable
 dhcp snooping alarm user-bind enable
 dhcp snooping alarm user-bind threshold 120
 dhcp snooping check mac-address enable
 dhcp snooping alarm mac-address enable
 dhcp snooping alarm mac-address threshold 120
 dhcp snooping alarm untrust-reply enable
 dhcp snooping alarm untrust-reply threshold 120
 dhcp snooping max-user-number 20
#
interface Ethernet2/0/2
 dhcp snooping trusted
#
```

# Run the **display dhcp snooping interface** command to view DHCP snooping information on an interface.

```
[RouterC] display dhcp snooping interface ethernet 2/0/0
 DHCP snooping running information for interface Ethernet2/0/0 :
 DHCP snooping                       : Enable
 Trusted interface                   : No
 Dhcp user max number                : 20
 Current dhcp user number            : 0
 Check dhcp-giaddr                   : Enable
 Check dhcp-chaddr                   : Enable
 Alarm dhcp-chaddr                   : Enable
 Alarm dhcp-chaddr threshold         : 120
 Discarded dhcp packets for check chaddr  : 0
 Check dhcp-request                  : Enable
 Alarm dhcp-request                  : Enable
 Alarm dhcp-request threshold        : 120
 Discarded dhcp packets for check request : 0
 Alarm dhcp-reply                    : Enable
 Alarm dhcp-reply threshold          : 120
 Discarded dhcp packets for check reply   : 0
[RouterC] display dhcp snooping interface ethernet 2/0/2
 DHCP snooping running information for interface Ethernet2/0/2 :
 DHCP snooping                       : Disable  (default)
 Trusted interface                   : Yes
 Dhcp user max number                : 512    (default)
 Current dhcp user number            : 0
 Check dhcp-giaddr                   : Disable  (default)
 Check dhcp-chaddr                   : Disable  (default)
 Alarm dhcp-chaddr                   : Disable  (default)
```

 Copyright © Huawei Technologies Co., Ltd. 

```
Check dhcp-request                : Disable  (default)
Alarm dhcp-request                : Disable  (default)
Alarm dhcp-reply                  : Disable  (default)
```

**----End**

## Configuration Files

RouterC configuration file

```
#
sysname RouterC
#
dhcp enable
#
dhcp snooping enable
arp dhcp-snooping-detect enable
#
interface Ethernet2/0/0
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check user-bind enable
 dhcp snooping alarm user-bind enable
 dhcp snooping alarm user-bind threshold 120
 dhcp snooping check mac-address enable
 dhcp snooping alarm mac-address enable
 dhcp snooping alarm mac-address threshold 120
 dhcp snooping alarm untrust-reply enable
 dhcp snooping alarm untrust-reply threshold 120
 dhcp snooping max-user-number 20
#
interface Ethernet2/0/1
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check user-bind enable
 dhcp snooping alarm user-bind enable
 dhcp snooping alarm user-bind threshold 120
 dhcp snooping check mac-address enable
 dhcp snooping alarm mac-address enable
 dhcp snooping alarm mac-address threshold 120
 dhcp snooping alarm untrust-reply enable
 dhcp snooping alarm untrust-reply threshold 120
 dhcp snooping max-user-number 20
#
interface Ethernet2/0/2
 dhcp snooping trusted
#
return
```

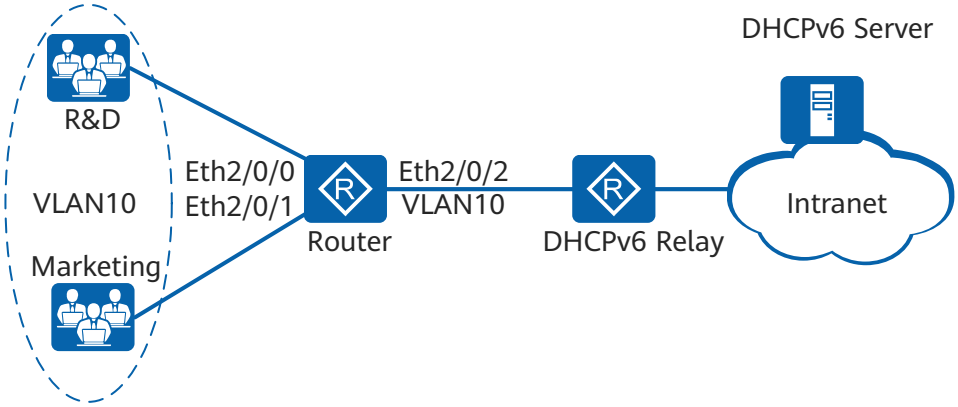
# 13.12.2 Example for Configuring LDRA to Detect Client Locations

## Networking Requirements

As shown in **Figure 13-9**, the R&D department and marketing department of a company connect to the Internet through the Router and obtain IPv6 addresses using DHCPv6. The company requires that the DHCPv6 server assigns different IP addresses, access control policies, and QoS policies to the clients in different departments.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 13-9** Networking diagram for configuring LDRA




## Configuration Roadmap

The configuration roadmap is as follows:

1. Enable DHCP snooping.
2. Enable LDRA. After LDRA is enabled on the Router, the Router can forward the client location information to the DHCPv6 server, and the DHCPv6 server can assign corresponding policies to the clients.

## Procedure

**Step 1** Create a VLAN and configure interfaces.

# Create VLAN 10 on the Router.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10
```

# Add interfaces Eth2/0/0, Eth2/0/1, and Eth2/0/2 to VLAN 10.

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type access
[Router-Ethernet2/0/0] port default vlan 10
[Router-Ethernet2/0/0] quit
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] port link-type access
[Router-Ethernet2/0/1] port default vlan 10
[Router-Ethernet2/0/1] quit
[Router] interface ethernet 2/0/2
[Router-Ethernet2/0/2] port link-type trunk
[Router-Ethernet2/0/2] port trunk allow-pass vlan 10
[Router-Ethernet2/0/2] quit
```

**Step 2** Enable DHCP snooping.

# Enable DHCP snooping globally.

```
[Router] dhcp enable
[Router] dhcp snooping enable
```

# Enable DHCP snooping on the user-side interfaces.

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] dhcp snooping enable
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router-Ethernet2/0/0] quit
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] dhcp snooping enable
[Router-Ethernet2/0/1] quit
```

# Set the status of the interface connecting to the DHCPv6 server to Trusted.

```
[Router] interface ethernet 2/0/2
[Router-Ethernet2/0/2] dhcp snooping trusted
[Router-Ethernet2/0/2] quit
```

**Step 3** Enable the LDRA.

# Enable the LDRA in VLAN 10.

```
[Router] vlan 10
[Router-vlan10] dhcpv6 snooping relay-information enable
```

# Disable the interfaces in VLAN 10 from generating DHCP snooping binding entries. After DHCP snooping is enabled, the interfaces will not restrict the number of online users.

```
[Router-vlan10] dhcp snooping enable no-user-binding
Warning: To execute no-user-binding will delete all dynamic binding table with the same vlan. Continue? [Y/N]y
[Router-vlan10] quit
```

**Step 4** Verify the configuration.

# Run the **display dhcp snooping configuration** command to verify the LDRA configuration.

```
[Router] display dhcp snooping configuration
#
dhcp snooping enable
#
vlan 10
 dhcp snooping enable no-user-binding
 dhcpv6 snooping relay-information enable
#
interface Ethernet2/0/0
 dhcp snooping enable
#
interface Ethernet2/0/1
 dhcp snooping enable
#
interface Ethernet2/0/2
 dhcp snooping trusted
#
```

**----End**

## Configuration Files

Router configuration file

```
#
 sysname Router
#
vlan batch 10
#
dhcp enable
#
dhcp snooping enable
#
vlan 10
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 dhcp snooping enable no-user-binding
 dhcpv6 snooping relay-information enable
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 10
 dhcp snooping enable
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 10
 dhcp snooping enable
#
interface Ethernet2/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 dhcp snooping trusted
#
return
```

# 13.13 Troubleshooting DHCP Snooping

## 13.13.1 DHCP Clients Cannot Go Online Due to DHCP Snooping

### Fault Description

The possible causes are as follows:

- The network-side interface connected to the DHCP server is not configured as the trusted interface.
- The number of DHCP clients connected to the user-side interface has reached the maximum value.

### Procedure

**Step 1** Check whether the trusted interface is correctly configured.

1. Run the **display dhcp snooping configuration** command to check in which VLANs and on which interfaces DHCP snooping is enabled and whether "Trusted interface" is displayed on the network-side interface.

   NOTE

   After DHCP snooping is enabled on an interface, the interface is an untrusted interface by default. When receiving messages from the network-side interfaces, the device processes only the DHCP Reply messages received on the trusted interface and discards those on untrusted interfaces. When receiving messages from user-side interfaces, the device forwards the messages only to the trusted interface.

2. Check whether the network-side interface on the DHCP server is the trusted interface. If it is not the trusted interface, run the **dhcp snooping trusted** command in the VLAN or interface view to configure the interface as a trusted interface.

**Step 2** If the interface is correctly configured, check whether the number of access DHCP clients reaches the threshold.

 Copyright © Huawei Technologies Co., Ltd. 

1. Run the **display dhcp snooping configuration** command to check whether "DHCP user max number: XX" is displayed globally, in the VLAN or on the user-side interface.

   NOTE

   If "DHCP user max number: XX" is not displayed, the default maximum number of DHCP clients is 512. The configured value takes preference.

   If you set the maximum value in the system view, VLAN view, and the interface view, the smallest value takes effect.

2. Run the **display dhcp snooping user-bind all** command to view the number of dynamic DHCP snooping entries on the DHCP snooping-enabled interface. If the number of entries on the interface has reached the maximum value, new DHCP clients cannot access the network.

**----End**

# 13.14 FAQ About DHCP Snooping

## 13.14.1 Can a Router Provide DHCP Snooping Function Without Using a LAN Card?

No, DHCP snooping function can only be provided by the LAN card.

To restrict source MAC addresses without a LAN card installed, the router can use Layer 2 ACL. However, Layer 2 ACL is not a replacement for DHCP snooping.

 Copyright © Huawei Technologies Co., Ltd. 

# 14 IPSG Configuration

## About This Chapter

This chapter describes how to configure IP source guard (IPSG) to check received IP packets against a binding table as a defense measure against source IP address spoofing attacks.

14.1 Overview of IPSG

14.2 Understanding IPSG

14.3 Application Scenarios for IPSG

14.4 Licensing Requirements and Limitations for IPSG

14.5 Default Settings for IPSG

14.6 Configuring IPSG

14.7 Configuration Examples for IPSG

14.8 Troubleshooting IPSG

14.9 FAQ About IPSG

## 14.1 Overview of IPSG

### Definition

IP Source Guard (IPSG) implements source IP address filtering based on Layer 2 interfaces to prevent malicious hosts from posing as authorized hosts by using authorized hosts' IP addresses. In addition, IPSG prevents unauthorized hosts from accessing or attacking networks with the IP addresses configured by themselves.

### Purpose

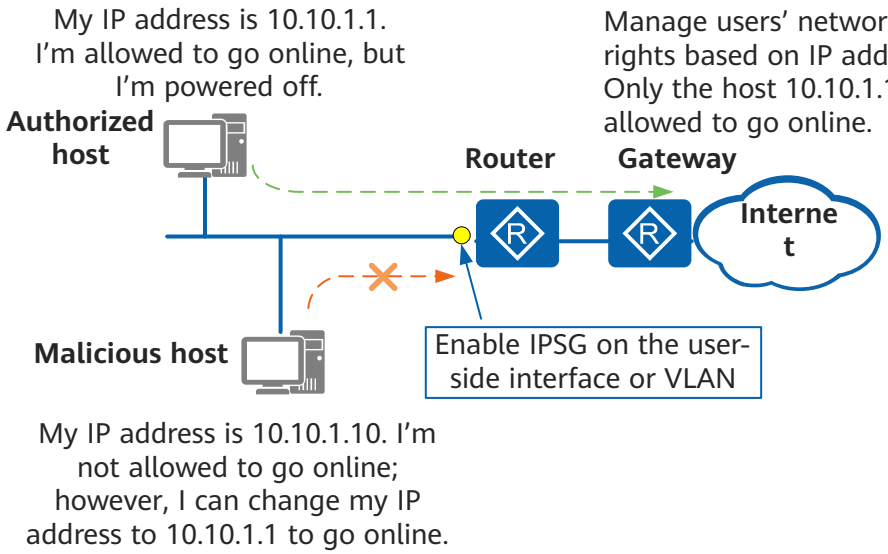
As networks continue to increase in scale, many attackers are forging source IP addresses to initiate network attacks (IP address spoofing attacks). Some attackers

 Copyright © Huawei Technologies Co., Ltd. 

steal the IP addresses of authorized users to obtain network access rights and access networks. As a result, authorized users are unable to access networks or sensitive information may be intercepted. IPSG provides a mechanism to effectively defend against IP address spoofing attacks.

Figure 14-1 illustrates how IPSG defends against attacks. A malicious host steals an authorized host's IP address to obtain network access rights. IPSG is configured on the device's user-side interface or VLAN, so the device checks the IP packets received by the interface and discards the packets from malicious hosts to prevent IP address spoofing attacks.

**Figure 14-1** IPSG is enabled on the network




# 14.2 Understanding IPSG

## 14.2.1 IPSG Fundamentals

IPSG checks IP packets on Layer 2 interfaces against a binding table that contains the bindings of source IP addresses, source MAC addresses, VLANs, and inbound interfaces. Only packets matching the binding table are forwarded, and other packets are discarded.

Table 14-1 describes two types of binding tables: static and dynamic binding tables.

**Table 14-1** Binding tables

| Type | Description | Applicable Scenario |
| --- | --- | --- |
| Static binding table | Manually configured using the **user-bind** command. | A network has a few hosts that use static IP addresses. |

 Copyright © Huawei Technologies Co., Ltd. 

| Type | Description | Applicable Scenario |
| --- | --- | --- |
| DHCP snooping dynamic binding table | After DHCP snooping is configured, hosts request IP addresses from the DHCP server. The device generates DHCP snooping dynamic binding entries according to the DHCP reply ACK packets returned by DHCP server. | A network has many hosts that obtain IP addresses from the DHCP server. |

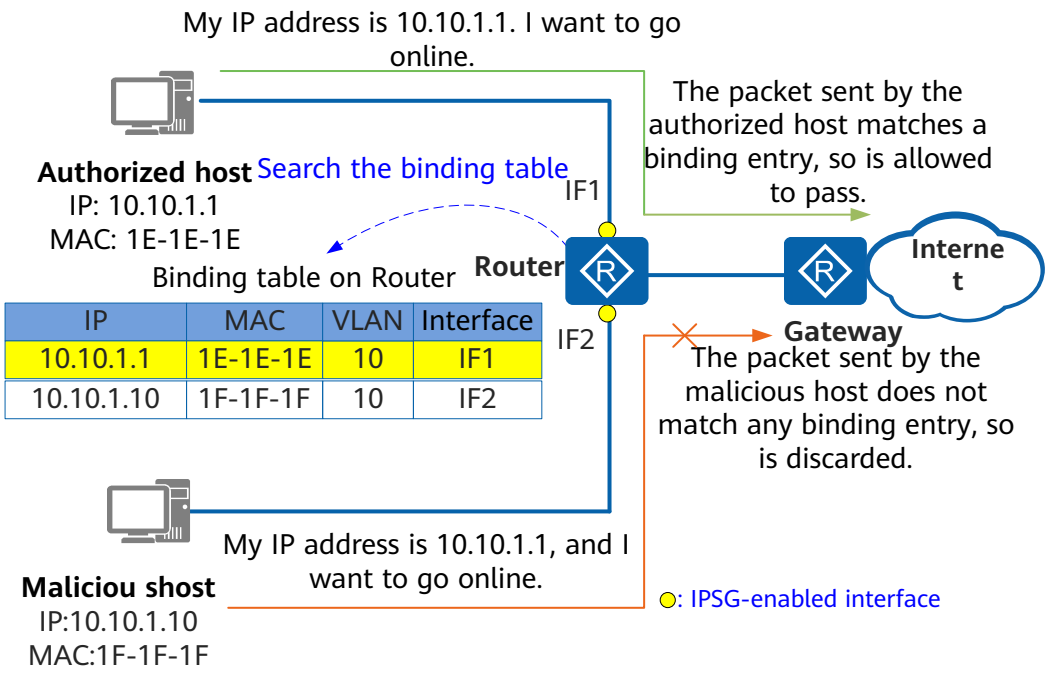
After the binding table is generated, the device forwards the packets from hosts only when the packets match binding entries, and discards the packets when the packets do not match binding entries. By default, if IPSG is enabled but no binding table is configured, the device discards all IP packets except DHCP Request packets.

**NOTE**

IPSG checks only the IP packets, but does not check non-IP packets such as ARP and PPPoE packets.

**Figure 14-2** illustrates IPSG working mechanism. When a malicious host uses an authorized host's IP address to send packets to the Router, the Router detects that the packets do not match binding entries, and then discards the packets.

**Figure 14-2** IPSG working mechanism




 Copyright © Huawei Technologies Co., Ltd. 

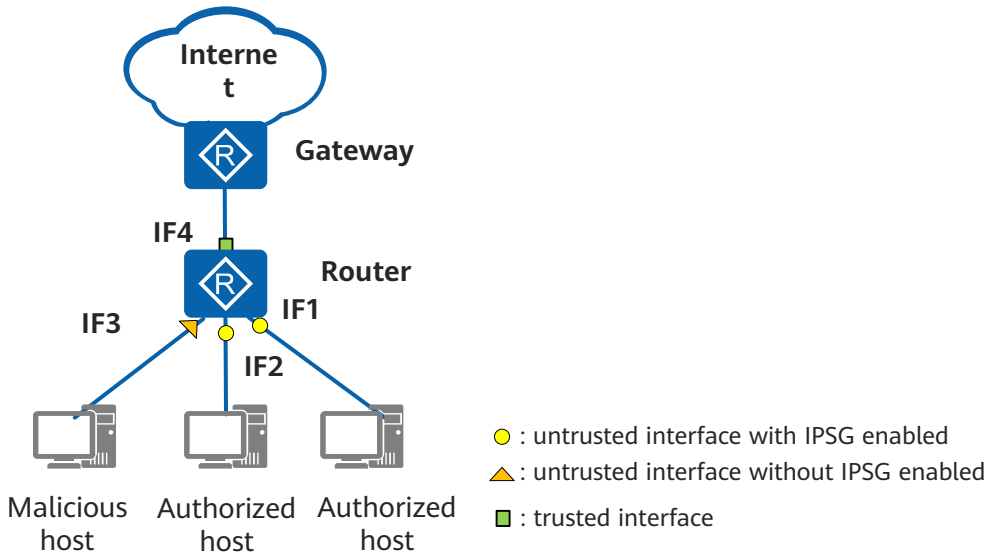
## IPSG Interface Roles

IPSG can only be configured on Layer 2 physical interfaces or in VLANs, and checks only the packets on the untrusted interfaces with IPSG enabled. IPSG considers all interfaces to be untrusted by default. Trusted interfaces are manually specified. IPSG trusted and untrusted interfaces are also used as trusted and untrusted interfaces in the DHCP snooping functions. In addition, the trusted and untrusted interfaces are also valid for IPSG based on a static binding table.

Figure 14-3 shows the IPSG interface roles:

- IF1 and IF2 are untrusted interfaces and have the IPSG function enabled. The device performs an IPSG check on the packets received by IF1 and IF2.
- IF3 is an untrusted interface and does not have the IPSG function enabled. The device does not perform an IPSG check on the packets received by IF3. Therefore, IF3 is prone to attacks.
- IF4 is the trusted interface, which is manually configured. The device does not perform an IPSG check on the packets received by IF4; however, IF4 is not prone to attacks. On a network with DHCP snooping configured, the interfaces directly or indirectly connected to a valid DHCP server are generally configured as trusted interfaces.

**Figure 14-3** IPSG interface roles




## IPSG Filtering

IPSG filters packets based on MAC addresses, IP addresses, VLAN IDs, and inbound interfaces.

- When a static binding entry is configured, all the four items must be specified.
- When a dynamic binding entry is configured, you can choose the check items. By default, IPSG checks packets against all the four options. Table 14-2 describes commonly used check methods. The usage of other combinations is similar to those in the table, and is not provided here.


Copyright © Huawei Technologies Co., Ltd.

**Table 14-2** IPSG filtering

| Option | Description |
| --- | --- |
| **In the interface view** | |
| Interface and Source IP address | In the interface view, the device validates the source IP addresses of packets, and forwards the packets only when the source IP addresses in packets match binding entries. |
| Interface and Source MAC address | In the interface view, the device validates the source MAC addresses of packets, and forwards the packets only when the source IP addresses in packets match binding entries. |
| Interface, Source IP address and source MAC address | In the interface view, the device validates the source IP and MAC addresses of packets, and forwards the packets only when the source IP and MAC addresses in packets match binding entries. |
| Interface, Source IP address and VLAN | In the interface view, the device validates the source IP addresses and VLANs of packets, and forwards the packets only when the source IP addresses and VLANs in packets match binding entries. |
| Interface, source MAC address and VLAN | In the interface view, the device validates the source MAC addresses and VLANs of packets, and forwards the packets only when the source MAC addresses and VLANs in packets match binding entries. |
| Interface, Source IP address, source MAC address, and VLAN | In the interface view, the device validates the source IP addresses, source MAC addresses, and VLANs of packets, and forwards the packets only when the source IP addresses, source MAC addresses, and VLANs in packets match binding entries. |
| **In the VLAN view** | |
| VLAN and Source IP address | In the VLAN view, the device validates the source IP addresses of packets, and forwards the packets only when the source IP addresses in packets match binding entries. |
| VLAN and Source MAC address | In the VLAN view, the device validates the source MAC addresses of packets, and forwards the packets only when the source MAC addresses in packets match binding entries. |
| VLAN, Source IP address and source MAC address | In the VLAN view, the device validates the source IP and MAC addresses of packets, and forwards the packets only when the source IP and MAC addresses in packets match binding entries. |

 Copyright © Huawei Technologies Co., Ltd. 

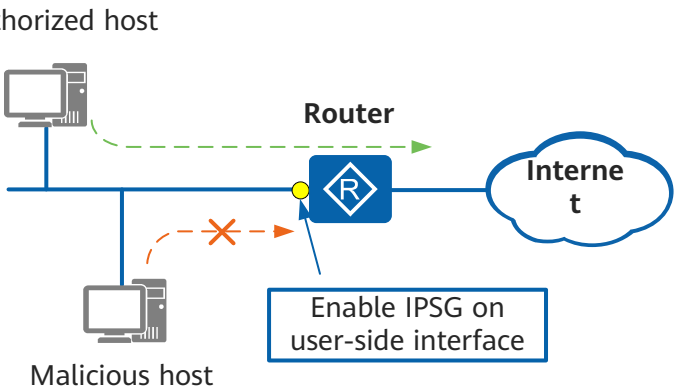
| Option | Description |
| --- | --- |
| VLAN, Source IP address and interface | In the VLAN view, the device validates the source IP addresses and interfaces of packets, and forwards the packets only when the source IP addresses and interfaces in packets match binding entries. |
| VLAN, source MAC address and interface | In the VLAN view, the device validates the source MAC addresses and interfaces of packets, and forwards the packets only when the source MAC addresses and interfaces in packets match binding entries. |
| VLAN, Source IP address, source MAC address and interface | In the VLAN view, the device validates the source IP addresses, source MAC addresses, and interfaces of packets, and forwards the packets only when the source IP addresses, source MAC addresses, and interfaces in packets match binding entries. |

## 14.2.2 IPSG Deployment

Generally, IPSG is configured on the interfaces or VLANs of the access device connected to users.

- As shown in **Figure 14-4**, after IPSG is enabled on the user-side interface of the device, the device performs an IPSG check on all IP packets received by this interface.

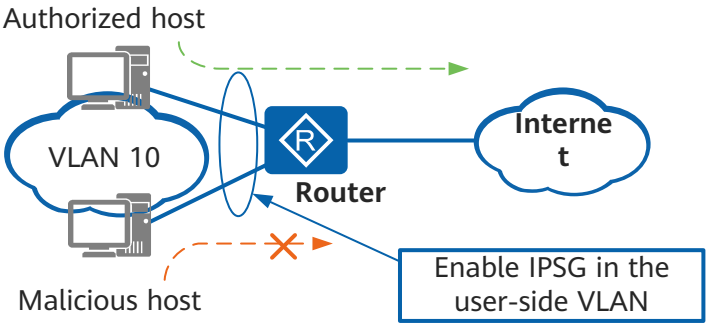
  **Figure 14-4** IPSG is enabled on an interface

- As shown in **Figure 14-5**, after IPSG is enabled on the user-side VLAN, the device performs an IPSG check on the IP packets received by all interfaces in this VLAN.

 Copyright © Huawei Technologies Co., Ltd. 

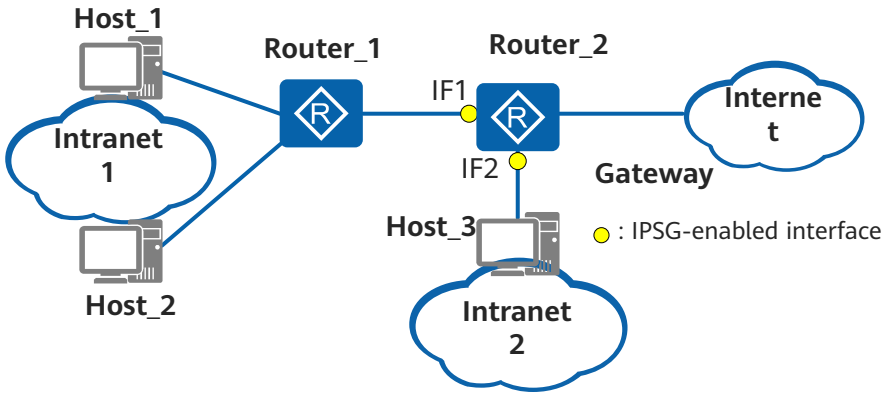
**Figure 14-5** IPSG is enabled in a VLAN




If the access device directly connected to users does not support IPSG, IPSG can be configured on the aggregation or core device, as shown in **Figure 14-6**.

- For example, Router_1 connected to intranet 1 does not support IPSG, so IPSG is configured on IF1 of Router_2 (a binding table needs to be built on Router_2 for the hosts in intranet 1). Router_1 does not support IPSG, so the packets from Router_1 may be IP address spoofing packets. IPSG configured on IF1 of Router_2 can block the attack and minimize the attack scope.
- IPSG also needs to be configured on IF2 of Router_2, which is connected to intranet 2; otherwise, intranet 2 is prone to IP address spoofing attacks.

**Figure 14-6** Multi-device environment




## 14.2.3 Comparison Between IPSG and Other Features

IPSG, Dynamic ARP Inspection (DAI), static ARP, and port security are network security technologies. This section describes the differences between **IPSG and DAI**, **IPSG and Static ARP**, **IPSG and Port Security**.

### IPSG and DAI

IPSG and DAI use binding tables (static or DHCP snooping binding tables) to filter packets. **Table 14-3** lists their differences.


Copyright © Huawei Technologies Co., Ltd.

**Table 14-3** Differences between IPSG and DAI

| Feature | Description | Usage Scenario |
| --- | --- | --- |
| IPSG | Filters IP packets by using binding tables. The device matches IP packets received by interfaces against binding entries, and forwards the IP packets matching the binding entries. | Prevent IP address spoofing attacks. For example, a malicious host steals an authorized host's IP address to access the network or initiate attacks. |
| DAI | Filters ARP packets by using binding tables. The device matches ARP packets received by interfaces against binding entries, and forwards the ARP packets matching the binding entries. | Prevent man-in-the-middle attacks. Man-in-the-middle attacks are generally initiated through ARP spoofing. That is, the attacker leads traffic to itself to intercept other hosts' information. |

IPSG cannot prevent address conflicts. For example, when a malicious host steals an online host's IP address, the ARP request packets sent by the malicious host will be sent to the online host through broadcast, causing an address conflict. Therefore, to prevent IP address conflicts, you can configure both IPSG and DAI.

For DAI configuration details, see **ARP Security Configuration** in the Huawei AR Series Access Routers Configuration Guide - Security.

## IPSG and Static ARP

Both IPSG based on a static binding table and static ARP support IP and MAC binding. **Table 14-4** lists their differences.

**Table 14-4** Differences between IPSG and static ARP

| Feature | Description | Usage Scenario |
| --- | --- | --- |
| IPSG | Builds a static binding table to bind IP addresses to MAC addresses. The device checks the packets received by interfaces, and forwards the packets matching the binding entries. | IPSG is generally configured on the access device connected to users or on the aggregation or core device to prevent IP address spoofing attacks from the intranet. For example, a malicious host steals an authorized host's IP address to access the network. |

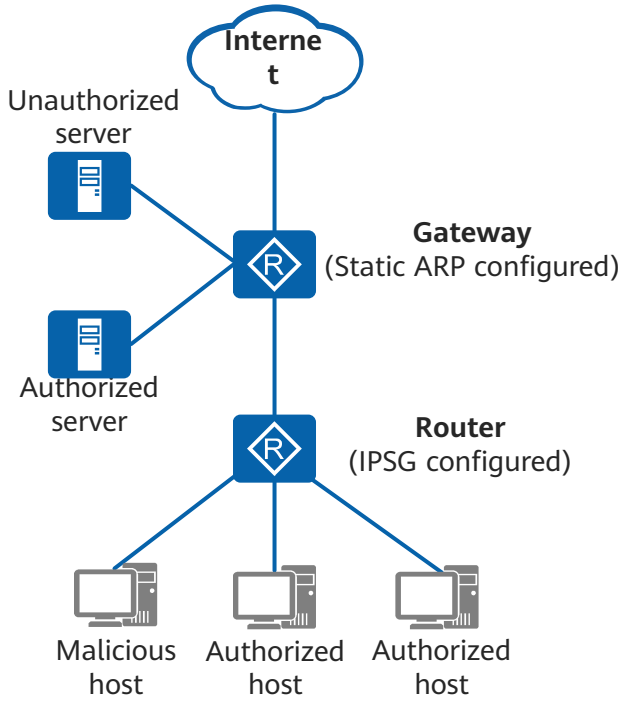
 Copyright © Huawei Technologies Co., Ltd. 

| Feature | Description | Usage Scenario |
| --- | --- | --- |
| Static ARP | Builds a static ARP table to bind IP addresses to MAC addresses. A static ARP table is not dynamically updated. The device processes received packets according to the static ARP table. | Generally, static ARP is configured on the gateway. The static ARP table stores the ARP entries of key servers to prevent ARP spoofing attacks and ensure normal communication between hosts and servers. |

**Figure 14-7** shows an example of IPSG and static ARP usage.

- IPSG is configured on the router to prevent malicious hosts from changing their own IP addresses or stealing authorized hosts' IP addresses to access the network.
- Static ARP entries of servers are configured on the gateway to prevent unauthorized servers from initiating ARP attacks or incorrectly updating ARP entries, so that hosts and authorized servers can communicate with each other normally.

**Figure 14-7** IPSG and Static ARP




The differences between IPSG and static ARP are as follows:

- **Static ARP cannot prevent IP address spoofing attacks.**

  Assume that IPSG is not configured on the router, and static ARP entries of hosts are configured on the gateway. When a malicious host steals an authorized host's IP address to access the Internet, the packet forwarding process is as follows:

 Copyright © Huawei Technologies Co., Ltd. 

a. The packet sent by the malicious host reaches the router.
b. The router forwards the packet to the gateway.
c. The gateway forwards the packet to the Internet.
d. The return packet from the Internet reaches the gateway.
e. The gateway searches for the static ARP entry according to the destination IP address (the IP address of the authorized host), and considers the MAC address corresponding to this IP address as the authorized host's MAC address. The gateway then encapsulates the packet and forwards the packet to the router.
f. The router forwards the packet to the authorized host according to the destination MAC address.

If the malicious host steals the IP address of an authorized host, static ARP can prevent the malicious from accessing the network by changing the IP address; however, the authorized host will receive a large number of invalid reply packets. If the malicious host keeps sending such packets, the online host will be attacked.

If the malicious host uses an idle IP address that has not been added to the static ARP table, the attack can be initiated successfully, and the return packets can be received by the malicious host. If you want to use static ARP to prevent IP address stealing, you need to add all the IP addresses on the network, including idle IP addresses to the static ARP table. This is a very time-consuming process.

In addition, static ARP is configured on the gateway, so IP address spoofing attacks on the network connected to the router cannot be prevented.

To prevent IP address spoofing attacks on an intranet, it is recommended that you configure IPSG on the router.

- **IPSG cannot prevent ARP spoofing attacks.**

  Assume that IPSG is configured on the router, and static ARP entries of hosts are not configured on the gateway.

  a. A malicious host steals an authorized host's IP address to send a fake ARP request packet to the router.
  b. The router forwards the packet to the gateway, and then the gateway incorrectly updates the ARP entry of the authorized host. In the ARP entry, the IP address belongs to the authorized host and the MAC address belongs to the malicious host.
  c. When the authorized host accesses the Internet, the Internet returns reply packets to the malicious host. As a result, the authorized host cannot go online.

     In addition, the packets sent by the Internet to the authorized host are intercepted by the malicious host.

  There are two methods to solve this problem. One method is to configure both IPSG on router and static ARP entries of hosts on the gateway; however, configuration and maintenance are complex for a network with a large number of hosts. Another method is to configure both IPSG and DAI on the router. The router matches IP and ARP packets received by interfaces against binding entries, and discards the ARP packets that do not match binding entries. The bogus ARP packets cannot reach the gateway, so the ARP entries will not be incorrectly modified.

 Copyright © Huawei Technologies Co., Ltd. 

For details on static ARP, see ARP Configuration in the Huawei AR Series Access Routers Configuration Guide - IP Services.

## IPSG and Port Security

Both IPSG based on a static binding table and port security support MAC and interface binding. **Table 14-5** lists their differences.

**Table 14-5** Differences between IPSG and port security

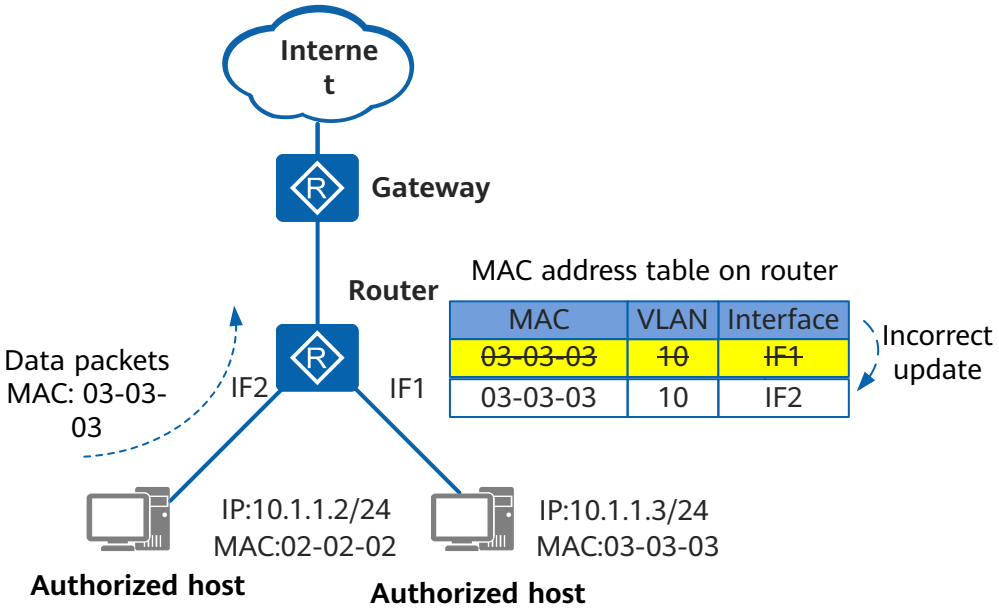
| Feature | Description | Usage Scenario |
| --- | --- | --- |
| IPSG | Binds MAC addresses to interfaces in the binding table so that a host can only go online through a fixed port. The hosts of which MAC addresses are not in the binding table cannot go online through the device.<br>The binding entries are manually configured. If a network has a large number of hosts, the configuration workload is heavy. | In addition to binding MAC addresses to interfaces, IPSG can bind IP addresses, MAC addresses, VLANs, and interfaces flexibly. IPSG prevents IP address spoofing attacks. For example, a malicious host steals an authorized host's IP address to access or attack the network. |
| Port security | Converts the limited number of dynamic MAC entries learned by interfaces into secure MAC entries, so that a host can only go online through a fixed port. The hosts of which MAC addresses are not in the MAC address table cannot go online through the device.<br>Secure MAC entries are dynamically generated. | Port security prevents access of unauthorized hosts and limits the number of access hosts. It is applicable to networks with a large number of hosts. |

Therefore, if you just want to prevent hosts with unauthorized MAC addresses from communicating with each other and a large number of hosts reside on the network, port security is recommended.

In addition, IPSG does not fix MAC entries, so it cannot prevent MAC address flapping caused by incorrect MAC entry updates. As shown in **Figure 14-8**, when a malicious host sends data (for example, bogus ARP packets) to the router by using an authorized host's MAC address, the router incorrectly updates the MAC address table. As a result, the malicious host can intercept the packets destined for the authorized host.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 14-8** Incorrect MAC address table update




To solve the MAC address flapping problem, you can configure the device to generate snooping MAC entries based on binding tables.

For details about port security, see **Port Security Configuration** in the Huawei AR Series Access Routers Configuration Guide - Security.

IPSG, DAI, static ARP, and port security resolve different issues and meet different requirements. To improve network security, it is recommended that you configure them according to your actual requirements.

# 14.3 Application Scenarios for IPSG

IPSG is applicable to campus networks to prevent hosts from accessing the network by changing their IP addresses to statically configured IP addresses and prevent unauthorized hosts from gaining network access.

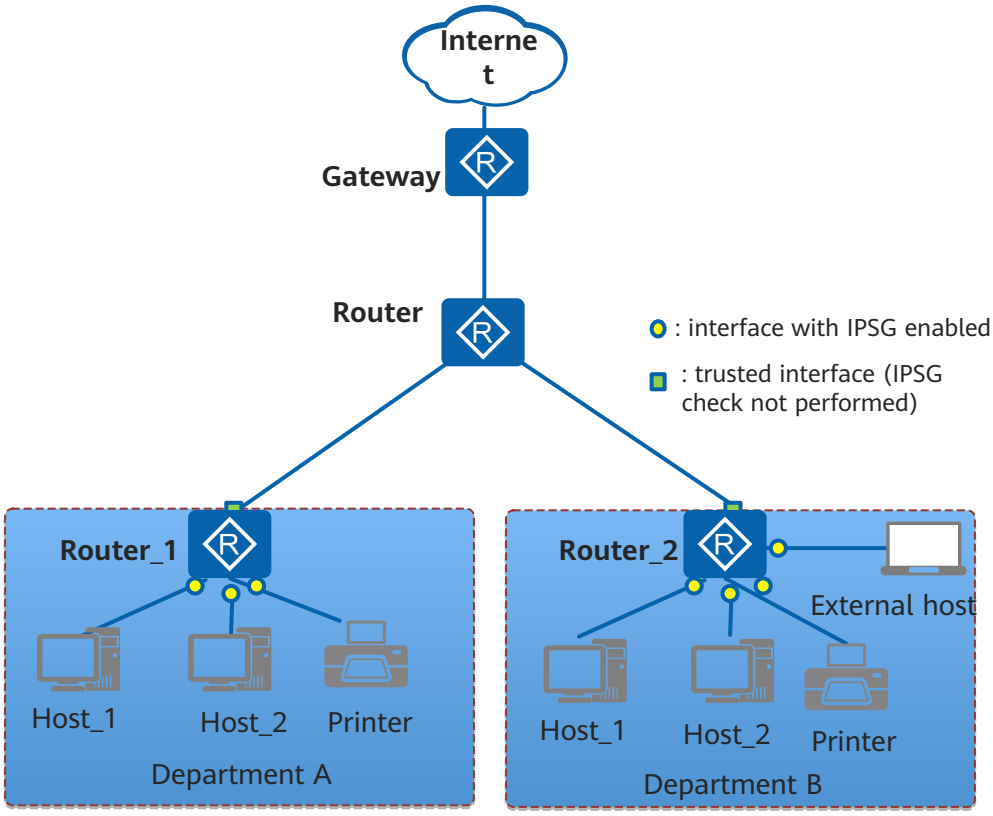
**Figure 14-9** shows a campus network. The actual network may have a different address assignment plan. For most campus networks:

- If a campus network is small, the hosts and printers use static IP addresses.
- If a campus network is large, the hosts obtain IP addresses through DHCP and some printers use static IP addresses.

IPSG is configured on the devices (Router_1 and Router_2) to which users connect.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 14-9** Typical IPSG networking




## Scenario 1: IPSG prevents hosts from accessing the network by changing their IP addresses to statically configured IP addresses

- Hosts can only use the IP addresses allocated by the DHCP server or static IP addresses configured by the administrator to access the network. If a host changes its IP address without permission, the host cannot access the network. This prevents hosts from obtaining network rights without permission.
- Static IP addresses configured for the printers can only be used by printers, and cannot be used by hosts to access the network.

## Scenario 2: IPSG prevents unauthorized hosts from gaining network access (static IP addresses are used on the network)

- Each host can only connect to a fixed port and cannot change the access location. The traffic rate on ports is limited.
- Users cannot access the intranet with their own computers. This prevents intranet resource leaks.

If hosts obtain IP addresses through DHCP, NAC (such as Portal authentication) can be configured to prevent unauthorized host access.

 Copyright © Huawei Technologies Co., Ltd. 

# 14.4 Licensing Requirements and Limitations for IPSG

## Involved Network Elements

Other network elements are not required.

## Licensing Requirements

IPSG is a basic feature of a router device and is not under license control.

## Feature Limitations

When deploying IPSG on the router, pay attention to the following:

- 4GE-2S, 4ES2G-S,4ES2GP-S and 9ES2 cards do not support IPSG.
- AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600 series support only Layer 3 traffic monitoring.

## Specifications

The IPSG static and dynamic binding entries share a limited number of resources. The total number of entries supported by different models is as follows:

- AR100&AR120&AR150&AR160&AR200 series: 128
- AR1200 series: 256
- AR2200 series: 1024 (AR2201-48FE, AR2202-48FE: 256)
- AR3200&AR3600 series: 1024

# 14.5 Default Settings for IPSG

Table 14-6 describes the default settings for IPSG. The default settings can be modified as required.

**Table 14-6** Default settings for IPSG

| Parameter | Default Setting |
| --- | --- |
| IP packet check | Disabled |
| IP packet check options | checks source IP address, source MAC address, interface, and VLAN |

# 14.6 Configuring IPSG


Copyright © Huawei Technologies Co., Ltd.

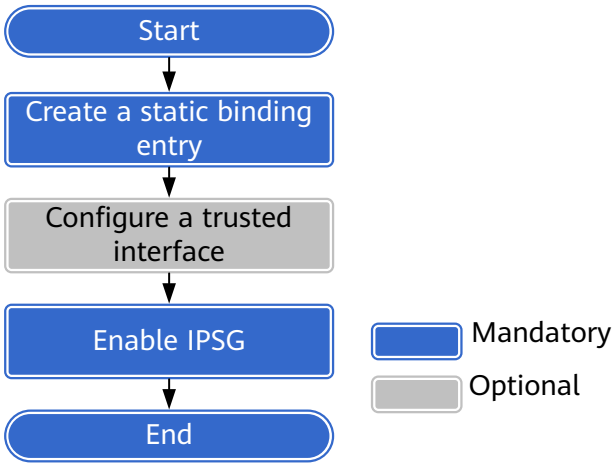
# 14.6.1 Configuring IPSG Based on a Static Binding Table

## Context

IPSG based on a static binding table filters IP packets received by untrusted interfaces, to prevent malicious hosts from stealing authorized hosts' IP addresses to access the network without permission. This function is applicable to a LAN where a small number of hosts reside and the hosts use static IP addresses.

## Configuration Procedure

**Figure 14-10** Configuration flowchart of IPSG based on a static binding table




Perform the following operations on the device to which users connect.

## Procedure

**Step 1** Create a static binding entry.

Static binding entries include IPv4 and IPv6 entries. Choose one type of entries according to your network type.

1. Run the **system-view** command to enter the system view.
2. Run the **user-bind static** { { **ip-address** | **ipv6-address** } { *start-ip* [ **to** *end-ip* ] } &<1-10> | **mac-address** *mac-address* } * [ **interface** *interface-type interface-number* ] [ **vlan** *vlan-id* [ **ce-vlan** *ce-vlan-id* ] ] command to configure a static binding entry.

   By default, no static binding entry exists.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

IPSG matches packets against all options in the static binding entry. Ensure that the created binding entry is correct and contains all the options to check. The device forwards the packets from hosts only when the packets match all options in the binding entry, and discards the packets not matching the binding entry.

The device can bind multiple IP addresses or IP address segments to the same interface or MAC address.

- If you need to bind discontinuous IP addresses, enter 1-10 IP addresses in *start-ip*. For example, you can run **user-bind static ip-address 192.168.1.2 192.168.1.5 192.168.1.12 interface ethernet 2/0/0** to bind multiple IP addresses to the same interface.
- If you need to bind continuous IP addresses, enter 1-10 IP address segments in *start-ip* **to** *end-ip*. When the keyword **to** is used, the IP address segments cannot overlap. For example, you can run **user-bind static ip-address 172.16.1.1 to 172.16.1.4 mac-address 0001-0001-0001** to bind multiple IP addresses to the same MAC address.

The AR100&AR120&AR150&AR160&AR200&AR1200 series do not support the keywords **ipv6-address** and **ce-vlan**.

If a static binding entry is incorrect or the network rights of a bound host have been changed, you can run the **undo user-bind static** [ **interface** *interface-type interface-number* | { **ip-address** | **ipv6-address** } { *start-ip* [ **to** *end-ip* ] } &<1-10> | **mac-address** *mac-address* | **vlan** *vlan-id* [ **ce-vlan** *ce-vlan-id* ] ] * command to delete the entry.

**Step 2** (Optional) Configure a trusted interface.

If the hosts on the network use static IP addresses, you do not need to configure trusted interfaces. However, if the upstream interface on the device belongs to an IPSG-enabled VLAN, configure this interface as the trusted interface; otherwise, the return packets are discarded because they do not match the binding entries. As a result, service will be interrupted. For the details about this problem, see **14.8.3 Service Is Abnormal Because the Upstream Interface Is Not Configured as a Trusted Interface**. After the upstream interface is configured as a trusted interface, the device forwards the packets received by the interface without checking them against the binding entries.

1. Run the **dhcp enable** command to enable DHCP globally.

   By default, DHCP is not enabled globally.
2. Run the **dhcp snooping enable** command to enable DHCP snooping globally.

   By default, DHCP snooping is disabled globally.
3. Configure the trusted interface.
   - Run the **dhcp snooping trusted interface** *interface-type interface-number* command in the VLAN view to configure the interface as the trusted interface.
   - Run the **dhcp snooping trusted** command in the interface view to configure the interface as the trusted interface.

   By default, interfaces are untrusted after DHCP snooping is enabled.

NOTE

The AR100&AR120&AR150&AR160&AR200&AR1200 series do not support trusted interfaces.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 3** Enable IPSG.

After a binding entry is created, IPSG does not take effect. IPSG takes effect only after it is enabled on the specified interface (user-side interface) or VLAN. There are two ways to enable IPSG.

- Enabling IPSG on an interface: IPSG checks all packets received by the interface against the binding entry. Choose this method if you need to check IP packets on the specified interfaces and trust other interfaces. In addition, this method is convenient if an interface belongs to multiple VLANs because you do not need to enable IPSG in each VLAN.
- Enabling IPSG in a VLAN: IPSG checks the packets received by all interfaces in the VLAN against the binding entry. Choose this method if you need to check IP packets in the specified VLANs and trust other VLANs. In addition, this method is convenient if multiple interfaces belong to the same VLAN because you do not need to enable IPSG on each interface.

NOTE

- If IPSG is enabled on an interface, IPSG takes effect only on this interface, and the device does not perform an IPSG check on other interfaces.
- If IPSG is enabled in a VLAN, IPSG takes effect in only this VLAN, and the device does not perform an IPSG check in other VLANs.

1. Enter the interface or VLAN view.
   - Run the **interface** *interface-type interface-number* command to enter the interface view.
   - Run the **vlan** *vlan-id* command to enter the VLAN view.
2. Run the **ip source check user-bind enable** command to enable IP packet check on the interface or in the VLAN.

   By default, IP packet check is disabled on interfaces or in VLANs.

**----End**

## Verifying the Configuration

- Run the **display ip source check user-bind** { **vlan** *vlan-id* | **interface** *interface-type interface-number* } command to view IPSG configurations.
- Run the **display dhcp static user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [ **verbose** ] command to view IPv4 static binding entries.

  Run the **display dhcpv6 static user-bind** { { **interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [ **verbose** ] command to view IPv6 static binding entries.

# 14.6.2 Configuring IPSG Based on a Dynamic Binding Table

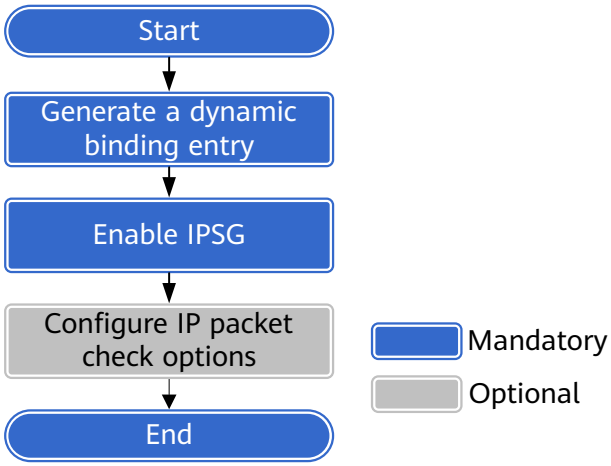
## Context

IPSG based on a dynamic binding table filters IP packets received by untrusted interfaces, to prevent malicious hosts from stealing authorized hosts' IP addresses to access the network without permission. This function is applicable to the LAN where a large number of hosts reside or the hosts obtain IP addresses through DHCP.

 Copyright © Huawei Technologies Co., Ltd. 

## Configuration Procedure

**Figure 14-11** Configuration flowchart of IPSG based on a dynamic binding table




Perform the following operations on the device to which users connect.

## Procedure

**Step 1** Create a dynamic binding entry.

Dynamic binding entries include IPv4 and IPv6 entries. Choose one type of entries according to your network type.

- If IPv4 or IPv6 hosts on the network obtain IP addresses through DHCP, DHCP snooping can be configured on the device to generate DHCP snooping dynamic binding entries for the hosts.
  a. Run the **system-view** command to enter the system view.
  b. Run the **dhcp enable** command to enable DHCP.
     By default, DHCP is disabled on a device.
  c. Run the **dhcp snooping enable** command to enable DHCP snooping globally.
     By default, DHCP snooping is disabled globally.
  d. Enter the VLAN or interface view.
     - Run the **vlan** *vlan-id* command to enter the VLAN view.
     - Run the **interface** *interface-type interface-number* command to enter the interface view.
  e. Run the **dhcp snooping enable** command to enable DHCP snooping in the VLAN or on the interface.
     By default, DHCP snooping is disabled in a VLAN or on an interface.
  f. Configure a trusted interface in either of the following ways:
     - Run the **dhcp snooping trusted interface** *interface-type interface-number* command in the VLAN view to configure the interfaces in the VLAN as trusted interfaces.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **dhcp snooping trusted** command in the interface view to configure the interface as a trusted interface.

By default, a DHCP snooping-enabled interface is an untrusted interface.

NOTE

The interface directly or indirectly connected to the server is generally configured as the trusted interface. After DHCP snooping is enabled and the trusted interface is configured, the interface on the user side generates dynamic binding entries based on DHCP ACK messages.

The AR100&AR120&AR150&AR160&AR200&AR1200 series do not support trusted interfaces. Before enabling DHCP snooping on an interface or in a VLAN, ensure that the DHCP relay or DHCP server function has been enabled on this interface or corresponding VLANIF interface; if they are not enabled, the device will not obtain the binding entries of users.

For details about DHCP snooping configuration, see **13 DHCP Snooping Configuration** in the Huawei AR Series Access Routers Configuration Guide - Security.

**Step 2** Enable IPSG.

After a binding entry is created, IPSG does not take effect. IPSG takes effect only after it is enabled on the specified interface (user-side interface) or VLAN. There are two ways to enable IPSG.

- Enabling IPSG on an interface: IPSG checks all packets received by the interface against the binding entry. Choose this method if you need to check IP packets on the specified interfaces and trust other interfaces. In addition, this method is convenient if an interface belongs to multiple VLANs because you do not need to enable IPSG in each VLAN.
- Enabling IPSG in a VLAN: IPSG checks the packets received by all interfaces in the VLAN against the binding entry. Choose this method if you need to check IP packets in the specified VLANs and trust other VLANs. In addition, this method is convenient if multiple interfaces belong to the same VLAN because you do not need to enable IPSG on each interface.

NOTE

- If IPSG is enabled on an interface, IPSG takes effect only on this interface, and the device does not perform an IPSG check on other interfaces.
- If IPSG is enabled in a VLAN, IPSG takes effect in only this VLAN, and the device does not perform an IPSG check in other VLANs.

1. Enter the interface or VLAN view.
   - Run the **interface** *interface-type interface-number* command to enter the interface view.
   - Run the **vlan** *vlan-id* command to enter the VLAN view.
2. Run the **ip source check user-bind enable** command to enable IP packet check on the interface or in the VLAN.

   By default, IP packet check is disabled on interfaces or in VLANs.

**Step 3** (Optional) Configure the IP packet check options.

- If IPSG has been enabled in a VLAN, run the **ip source check user-bind check-item** { **ip-address** | **mac-address** | **interface** }* command in the VLAN view to configure the IP packet check options.

 Copyright © Huawei Technologies Co., Ltd. 

- If IPSG has been enabled on an interface, run the **ip source check user-bind check-item** { **ip-address** | **mac-address** | **vlan** }* command in the interface view to configure the IP packet check options.

By default, the IP packet check options include IP address, MAC address, VLAN, and interface. If some options are trustable or unfixed (for example, packets from hosts may be received by different interfaces), you can perform this step. The default values are recommended.

**----End**

### Verifying the Configuration

- View the IPSG configuration.

  Run the **display ip source check user-bind** { **vlan** *vlan-id* | **interface** *interface-type interface-number* } command to view IPSG configurations.
- View the dynamic binding entries and status.
  - Run the **display dhcp snooping user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* }* | **all** } [ **verbose** ] command to view DHCP snooping dynamic binding entries.
  - Run the **display dhcpv6 snooping user-bind** { { **interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [ **verbose** ] command to view DHCPv6 snooping dynamic binding entries.

# 14.7 Configuration Examples for IPSG

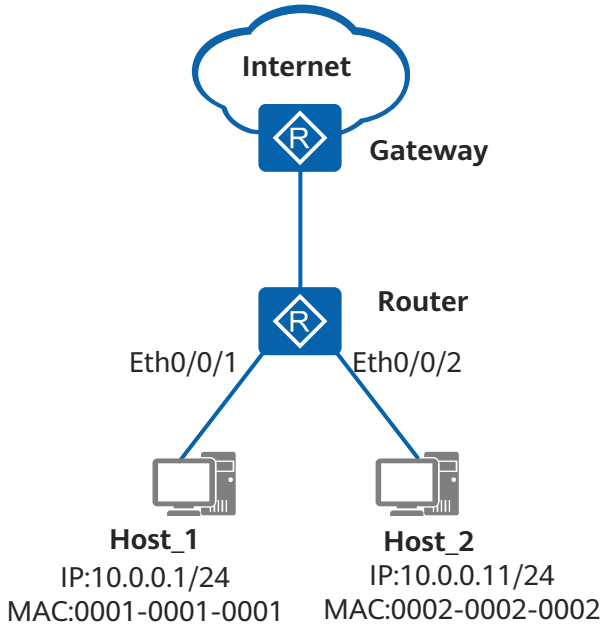
## 14.7.1 Example for Configuring IPSG Based on the Static Binding Table to Prevent Host to Use the IP Address of Another Host without Permission

### Networking Requirements

As shown in **Figure 14-12**, hosts access the enterprise internet through the Router. The gateway is the egress device of the enterprise internet. The hosts use static IP addresses. The administrator requires that the hosts can only use fixed IP addresses to access the internet. Users are not allowed to use the IP address of another host without permission to access the internet.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 14-12** Configuring IPSG based on the static binding table to prevent host to use the IP address of another host without permission




## Configuration Roadmap

The requirement of the administrator can be met by configuring IPSG on the Router. The configuration roadmap is as follows:

1. Configure static binding entries for Host_1 and Host_2 to fix the bindings between IP addresses and MAC addresses of the hosts.
2. Enable IPSG on the interfaces connected to user hosts so that the hosts can only use the fixed IP addresses to go online.

## Procedure

**Step 1** Create static binding entries for Host_1 and Host_2.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001
[Router] user-bind static ip-address 10.0.0.11 mac-address 0002-0002-0002
```

**Step 2** Enable IPSG.

# Enable IPSG on Eth0/0/1 connected to Host_1.

```
[Router] interface ethernet 0/0/1
[Router-Ethernet0/0/1] ip source check user-bind enable
[Router-Ethernet0/0/1] quit
```

# Enable IPSG on Eth0/0/2 connected to Host_2.

```
[Router] interface ethernet 0/0/2
[Router-Ethernet0/0/2] ip source check user-bind enable
[Router-Ethernet0/0/2] quit
```

**Step 3** Verify the configuration.

 Copyright © Huawei Technologies Co., Ltd. 

Run the **display dhcp static user-bind all** command on the Router to view static binding entries.

```
[Router] display dhcp static user-bind all
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address                MAC Address     VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
10.0.0.1                  0001-0001-0001  --  /--  /--    --
10.0.0.11                 0002-0002-0002  --  /--  /--    --
--------------------------------------------------------------------------------
Print count:          2         Total count:          2
```

Host_1 and Host_2 can access the internet using the statically configured IP addresses, and cannot access the internet after changing their IP addresses.

**----End**

## Configuration Files

Router configuration file

```
#
sysname Router
#
user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001
user-bind static ip-address 10.0.0.11 mac-address 0002-0002-0002
#
interface Ethernet0/0/1
 ip source check user-bind enable
#
interface Ethernet0/0/2
 ip source check user-bind enable
#
return
```

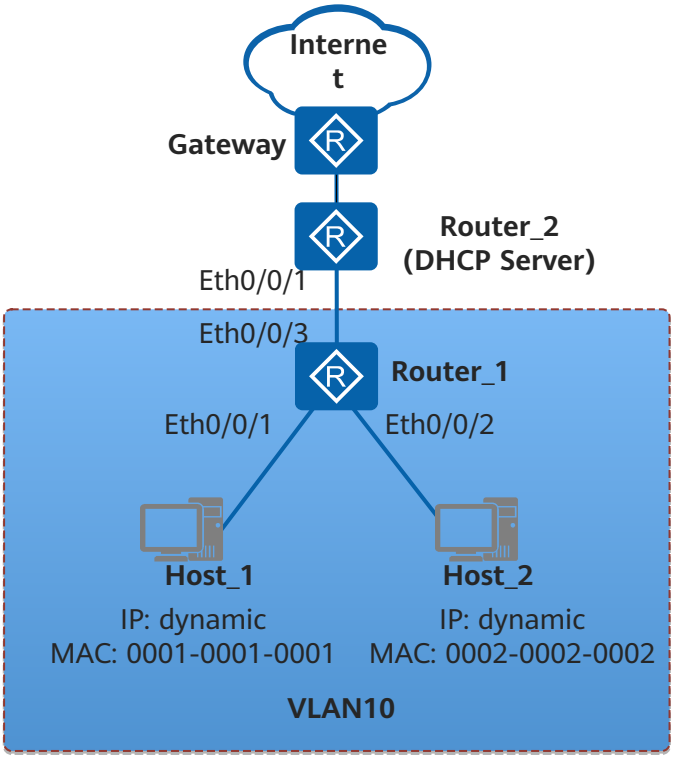
# 14.7.2 Example for Configuring IPSG Based on the DHCP Snooping Dynamic Binding Table to Prevent Host to Use the IP Address of Another Host without Permission

## Networking Requirements

As shown in **Figure 14-13**, hosts access the enterprise internet through Router_1, and Router_2 functions as a DHCP server to allocate IP addresses to the hosts. The gateway is the egress device of the enterprise internet. The administrator requires that the hosts use dynamically allocated IP addresses. The hosts cannot change their IP addresses to statically configured IP addresses to access the internet.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 14-13** Configuring IPSG based on the DHCP snooping dynamic binding table to prevent host to use the IP address of another host without permission




## Configuration Roadmap

The requirement of the administrator can be met by configuring IPSG. The configuration roadmap is as follows:

1. Configure the DHCP server (IP address pool 10.1.1.0/24) on Router_2 to allocate IP addresses to hosts.
2. Configure DHCP snooping on Router_1. Then the hosts can obtain IP addresses from the valid DHCP server, and the DHCP server can generate DHCP snooping dynamic binding entries, which record the bindings of IP addresses, MAC addresses, VLANs, and interfaces of hosts.
3. Enable IPSG in the VLAN to which the hosts belong to prevent the hosts from accessing the internet with changed IP addresses.

## Procedure

**Step 1** Configure the DHCP server on Router_2.

```
<Huawei> system-view
[Huawei] sysname Router_2
[Router_2] vlan batch 10
[Router_2] interface ethernet 0/0/1
[Router_2-Ethernet0/0/1] port link-type trunk
[Router_2-Ethernet0/0/1] port trunk allow-pass vlan 10
[Router_2-Ethernet0/0/1] quit
[Router_2] dhcp enable
[Router_2] ip pool 10
[Router_2-ip-pool-10] network 10.1.1.0 mask 24
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router_2-ip-pool-10] gateway-list 10.1.1.1
[Router_2-ip-pool-10] quit
[Router_2] interface vlanif 10
[Router_2-Vlanif10] ip address 10.1.1.1 255.255.255.0
[Router_2-Vlanif10] dhcp select global
[Router_2-Vlanif10] quit
```

**Step 2** Configure DHCP snooping on Router_1.

# Specify the VLAN to which the interfaces belong.

```
<Huawei> system-view
[Huawei] sysname Router_1
[Router_1] vlan batch 10
[Router_1] interface ethernet 0/0/1
[Router_1-Ethernet0/0/1] port link-type access
[Router_1-Ethernet0/0/1] port default vlan 10
[Router_1-Ethernet0/0/1] quit
[Router_1] interface ethernet 0/0/2
[Router_1-Ethernet0/0/2] port link-type access
[Router_1-Ethernet0/0/2] port default vlan 10
[Router_1-Ethernet0/0/2] quit
[Router_1] interface ethernet 0/0/3
[Router_1-Ethernet0/0/3] port link-type trunk
[Router_1-Ethernet0/0/3] port trunk allow-pass vlan 10
[Router_1-Ethernet0/0/3] quit
```

# Enable DHCP snooping and configure Eth0/0/3 connected to the DHCP server as a trusted interface.

```
[Router_1] dhcp enable
[Router_1] dhcp snooping enable
[Router_1] vlan 10
[Router_1-vlan10] dhcp snooping enable
[Router_1-vlan10] dhcp snooping trusted interface ethernet 0/0/3
```

**Step 3** Enable IPSG in VLAN 10 on Router_1.

```
[Router_1-vlan10] ip source check user-bind enable
[Router_1-vlan10] quit
```

**Step 4** Verify the configuration.

# After the hosts go online, run the **display dhcp snooping user-bind all** command on Router_1 to view dynamic binding entries of the hosts.

```
[Router_1] display dhcp snooping user-bind all
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address      MAC Address     VSI/VLAN(O/I/P) Interface      Lease
--------------------------------------------------------------------------------
10.1.1.254      0001-0001-0001  --  /10  /--    Eth0/0/1       2014.08.17-07:31
10.1.1.253      0002-0002-0002  --  /10  /--    Eth0/0/2       2014.08.17-07:34
--------------------------------------------------------------------------------
print count:     2     total count:     2
```

# The hosts can access the internet using the IP addresses dynamically allocated by the DHCP server. After the dynamic IP addresses of the hosts are changed to statically configured IP addresses that are different from the dynamic ones, the hosts cannot access the internet.

**----End**

## Configuration Files

- Router_1 configuration file

```
#
sysname Router_1
```

```
#
vlan batch 10
#
dhcp enable
#
dhcp snooping enable
#
vlan 10
 dhcp snooping enable
 dhcp snooping trusted interface Ethernet0/0/3
 ip source check user-bind enable
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

- Configuration file of Router_2

```
#
sysname Router_2
#
vlan batch 10
#
dhcp enable
#
ip pool 10
 gateway-list 10.1.1.1
 network 10.1.1.0 mask 255.255.255.0
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 dhcp select global
#
interface Ethernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

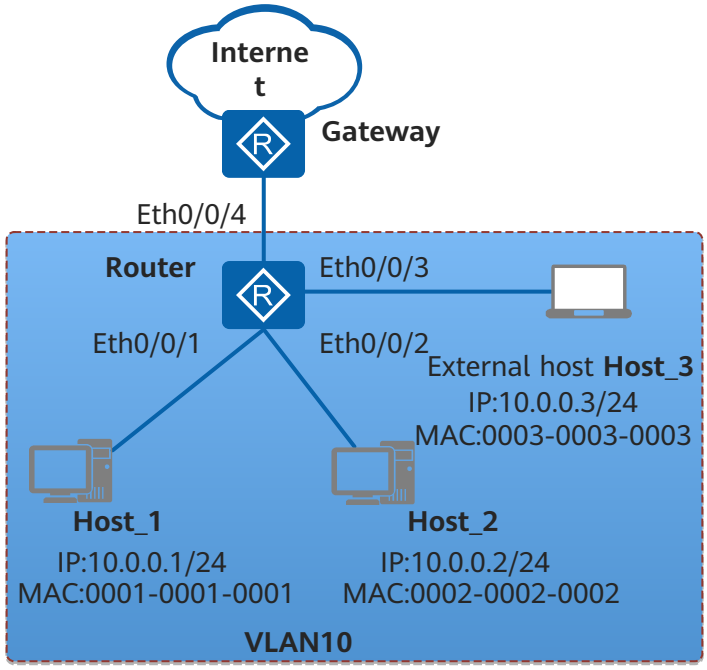
# 14.7.3 Example for Configuring IPSG Based on the Static Binding Table to Prevent Unauthorized Hosts from Accessing the intranet

## Networking Requirements

As shown in **Figure 14-14**, hosts access the enterprise intranet through the router. The gateway is the egress device of the enterprise intranet. The hosts use static IP addresses. The administrator has configured interface rate limiting on the router, and requires that the hosts use fixed IP addresses to access the intranet through fixed ports. To ensure network security, the administrator does not allow external hosts to access the intranet without permission.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 14-14** Configuring IPSG based on the static binding table to prevent unauthorized hosts from accessing the intranet




## Configuration Roadmap

The requirement of the administrator can be met by configuring IPSG on the Router. The configuration roadmap is as follows:

1. Specify the VLAN to which the interfaces belong.
2. Configure static binding entries for Host_1 and Host_2 to fix the bindings between IP addresses, MAC addresses, and interfaces.
3. Configure Eth0/0/4 as a trusted interface. The Router does not perform an IPSG check on the packets received by this trusted interface, so the packets returned by the gateway will not be discarded.
4. Enable IPSG in the VLAN connected to user hosts so that Host_1 and Host_2 access the intranet using fixed IP addresses through fixed ports. In addition, external host Host_3 cannot access the intranet.

## Procedure

**Step 1** Specify the VLAN to which the interfaces belong.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10
[Router] interface ethernet 0/0/1
[Router-Ethernet0/0/1] port link-type access
[Router-Ethernet0/0/1] port default vlan 10
[Router-Ethernet0/0/1] quit
[Router] interface ethernet 0/0/2
[Router-Ethernet0/0/2] port link-type access
[Router-Ethernet0/0/2] port default vlan 10
[Router-Ethernet0/0/2] quit
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router] interface ethernet 0/0/3
[Router-Ethernet0/0/3] port link-type access
[Router-Ethernet0/0/3] port default vlan 10
[Router-Ethernet0/0/3] quit
[Router] interface ethernet 0/0/4
[Router-Ethernet0/0/4] port link-type trunk
[Router-Ethernet0/0/4] port trunk allow-pass vlan 10
[Router-Ethernet0/0/4] quit
```

**Step 2** Create static binding entries for Host_1 and Host_2.

```
[Router] user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001 interface ethernet 0/0/1
[Router] user-bind static ip-address 10.0.0.2 mac-address 0002-0002-0002 interface ethernet 0/0/2
```

**Step 3** Configure the upstream interface Eth0/0/4 as a trusted interface.

```
[Router] dhcp enable
[Router] dhcp snooping enable
[Router] interface ethernet 0/0/4
[Router-Ethernet0/0/4] dhcp snooping trusted
[Router-Ethernet0/0/4] quit
```

**Step 4** Enable IPSG in VLAN 10 connected to hosts.

```
[Router] vlan 10
[Router-vlan10] ip source check user-bind enable
[Router-vlan10] quit
```

**Step 5** Verify the configuration.

# Run the **display dhcp static user-bind all** command on the Router to view binding entries of Host_1 and Host_2.

```
[Router] display dhcp static user-bind all
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address                MAC Address     VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
10.0.0.1                  0001-0001-0001  --  /--  /--    Eth0/0/1
10.0.0.2                  0002-0002-0002  --  /--  /--    Eth0/0/2
--------------------------------------------------------------------------------
Print count:          2         Total count:          2
```

# Host_1 and Host_2 can access the intranet. After the IP addresses of the hosts are changed or the hosts connect to other interfaces, they cannot access the intranet.

# When Host_3 with IP address 10.0.0.3 connects to Eth0/0/3, Host_3 cannot access the intranet, indicating that external hosts cannot access the intranet without permission. If Host_3 needs to access the intranet, add the entry of Host_3 to the static binding table.

**----End**

## Configuration Files

router configuration file

```
#
sysname Router
#
vlan batch 10
#
dhcp enable
#
dhcp snooping enable
user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001 interface Ethernet0/0/1
user-bind static ip-address 10.0.0.2 mac-address 0002-0002-0002 interface Ethernet0/0/2
```

 Copyright © Huawei Technologies Co., Ltd. 

```
#
vlan 10
 ip source check user-bind enable
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 10
#
interface Ethernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 10
 dhcp snooping trusted
#
return
```

# 14.8 Troubleshooting IPSG

## 14.8.1 IPSG Does Not Take Effect Because IPSG Is Not Enabled on the Interface or VLAN

### Fault Description

Binding entries have been generated, but the IPSG function does not take effect.

### Procedure

**Step 1** Check whether the IPSG function is enabled on the specified interface or VLAN.

After a binding entry is created, IPSG does not take effect. IPSG takes effect only after it is enabled on the specified interface or VLAN.

You can enable IPSG on the interface or in the VLAN. The differences are as follows:

- Enabling IPSG on an interface: IPSG checks all packets received by the interface against the binding entry. Choose this method if you need to check IP packets on the specified interfaces and trust other interfaces. In addition, this method is convenient if an interface belongs to multiple VLANs because you do not need to enable IPSG in each VLAN.
- Enabling IPSG in a VLAN: IPSG checks the packets received by all interfaces in the VLAN against the binding entry. Choose this method if you need to check IP packets in the specified VLANs and trust other VLANs. In addition, this method is convenient if multiple interfaces belong to the same VLAN because you do not need to enable IPSG on each interface.

IPSG takes effect only on the interface or VLAN where it is enabled, and IPSG check is not performed on the interfaces or VALNs without IPSG enabled.

 Copyright © Huawei Technologies Co., Ltd. 

Therefore, if IPSG does not take effect on an interface or in a VLAN, the IPSG function may not be enabled on this interface or in this VLAN.

**Step 2** Run the **display ip source check user-bind** { **vlan** *vlan-id* | **interface** *interface-type interface-number* } command to check whether IPSG is enabled on the interface or VLAN connected to access users.

**Step 3** If IPSG is not enabled on the interface, run the **display this** command in the VLAN view to check whether IPSG is enabled in the VLAN connected to access users.

**Step 4** If IPSG is neither enabled on the interface nor enabled in the VLAN ("ip source check user-bind enable" not displayed in the command output), run the **ip source check user-bind enable** command in the interface or VLAN view to enable IPSG.

**----End**

## 14.8.2 An Authorized Host Cannot Go Online Due to the Incorrect Static Binding Entry

### Fault Description

A static binding entry has been created for the host and IPSG has been enabled; however, the authorized host cannot go online.

### Procedure

**Step 1** Check whether the binding entry is correct.

Run the **display dhcp static user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } command to view static binding entries.

The binding entries may be incorrect, so the authorized host cannot go online.

- If the binding entry of the host is not in the binding table, add the host's binding entry to the binding table. The router allows the packets from a host to pass only when the host's binding entry exists in the binding table.
- If the host's entry exists in the binding table, check whether the MAC address in the entry is the same as the host's MAC address. If the network card of the host is replaced, the MAC address in the entry may not be updated in a timely manner. If so, delete the entry and configure a new binding entry for the host.
- If the host's binding entry exists in the binding table, check whether the entry contains VLAN information. If so, run the **display vlan** command to check whether the interface connected to the host has been added to the VLAN. The router allows the packets from a host to pass only when the interface connected to this host has been added to the VLAN.

**Step 2** Add a binding entry.

Run the **user-bind static** { { **ip-address** | **ipv6-address** } { *start-ip* [ **to** *end-ip* ] } &<1-10> | **mac-address** *mac-address* } * [ **interface** *interface-type interface-number* ] [ **vlan** *vlan-id* [ **ce-vlan** *ce-vlan-id* ] ] command.

**Step 3** Delete a binding entry.

 Copyright © Huawei Technologies Co., Ltd. 

Run the **undo user-bind static** [ **interface** *interface-type interface-number* | { **ip-address** | **ipv6-address** } { *start-ip* [ **to** *end-ip* ] } &<1-10> | **mac-address** *mac-address* | **vlan** *vlan-id* [ **ce-vlan** *ce-vlan-id* ] ] * command.

NOTE

The AR100&AR120&AR150&AR160&AR200&AR1200 series do not support the keywords **ipv6-address** and **ce-vlan**.

**----End**

# 14.8.3 Service Is Abnormal Because the Upstream Interface Is Not Configured as a Trusted Interface

## Fault Description

After IPSG is enabled in a VLAN, the hosts in the VLAN cannot access the Internet. Service on the hosts is abnormal.

## Procedure

**Step 1** Check whether the upstream interface belongs to the VLAN with IPSG enabled.

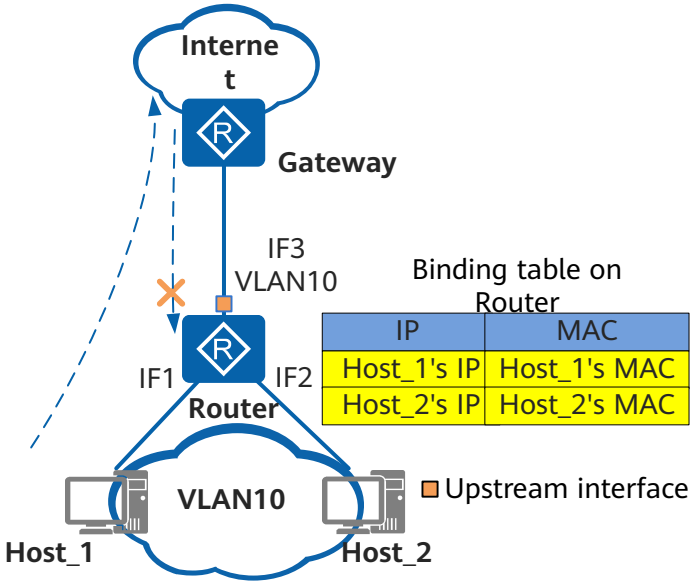
If the upstream interface belongs to the VLAN, configure this interface as the trusted interface; otherwise, the return packets are discarded because they do not match the binding entries. As a result, user service is interrupted.

As shown in **Figure 14-15**, Host_1 and Host_2 belong to VLAN 10. IF3 allows the packets of VLAN 10 to pass. The static binding entries are configured on the router for Host_1 and Host_2, and IPSG is enabled in VLAN 10. The hosts can communicate with each other, but cannot access the Internet. Host_1 is used as an example here to describe the fault symptom:

- Host_1 sends a packet to the Internet. When the packet reaches IF1 of the router, the router detects that the packet matches a binding entry, and forwards it.
- The Internet returns a packet to Host_1. When the packet reaches IF3, which belongs to VLAN 10, the router detects that the packet does not match any binding entry, and discards the packet.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 14-15** Service is abnormal because the upstream interface is not configured as a trusted interface




**Step 2** Procedure.

1. Run the **system-view** command to enter the system view.
2. Run the **dhcp enable** command to enable DHCP globally.
3. Run the **dhcp snooping enable** command to enable DHCP snooping globally.
4. Run the **interface** *interface-type interface-number* command to enter the IF3 interface view.
5. Run the **dhcp snooping trusted** command to configure IF3 as a trusted interface.

**----End**

## 14.8.4 Service Is Interrupted After IPSG Is Enabled on the Upstream Interface

### Fault Description

After IPSG is enabled on an interface, all hosts on the interface cannot access the Internet. Service on the hosts is abnormal.

### Procedure

**Step 1** Check whether IPSG has been enabled on an upstream interface.

Generally, IPSG is enabled on the user-side interface, namely, the downstream interface. If IPSG is enabled on the upstream interface, the packets returned by the gateway may be discarded. As a result, user service is interrupted.

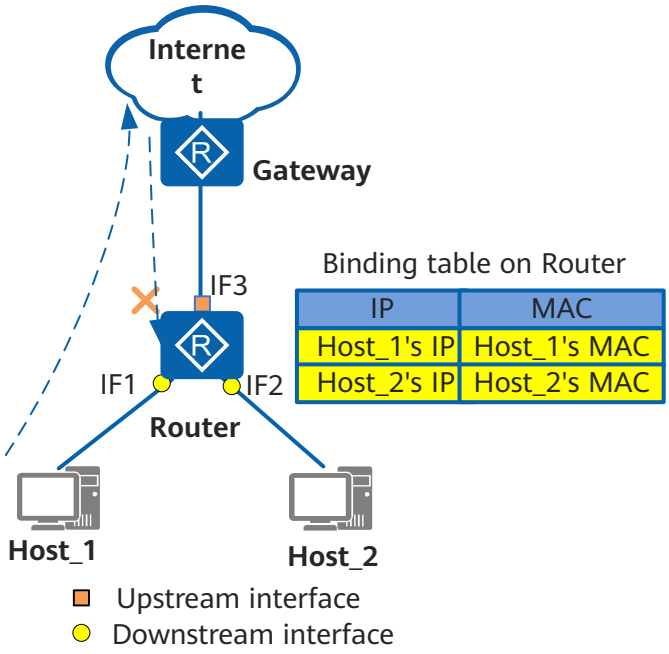
As shown in **Figure 14-16**, after static binding entries are configured on the router for Host_1 and Host_2 and IPSG is enabled on IF1, IF2, and IF3, the hosts cannot

 Copyright © Huawei Technologies Co., Ltd. 

access the Internet, but they can communicate with each other. Host_1 is used as an example here to describe the fault symptom:

- Host_1 sends a packet to the Internet. When the packet reaches IF1 of the router, the router detects that the packet matches a binding entry, and forwards it.
- The Internet returns a packet to Host_1. When the packet reaches IF3, the router detects that the packet does not match any binding entry, and discards the packet.

**Figure 14-16** Service is interrupted after IPSG is enabled on the upstream interface




**Step 2** Procedure.

1. Run the **display ip source check user-bind interface** *interface-type interface-number* command to check whether IPSG is enabled on the upstream interface IF3.
2. If "ip source check user-bind enable" is displayed, IPSG has been enabled on the upstream interface. Run the **undo ip source check user-bind enable** command in the interface view to disable IPSG on upstream interface IF3.

**----End**

## 14.8.5 Unbound Hosts Can Go Online After IP and MAC Bindings Are Configured

### Fault Description

After IP and MAC bindings are configured, the unbound hosts can go online.

 Copyright © Huawei Technologies Co., Ltd. 

## Procedure

**Step 1** Check whether static binding entries have been configured.

Run the **display dhcp static user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } command to view static binding entries.

If no static binding entries exist, the IP addresses and MAC addresses may not be correctly bound. Check whether the IP addresses and MAC addresses are bound using the **arp static** *ip-address mac-address* command. This command configures static ARP, but not IPSG. Static ARP cannot prevent unbound hosts from going online.

**Step 2** Configure static binding entries.

Run the **user-bind static** { { **ip-address** | **ipv6-address** } { *start-ip* [ **to** *end-ip* ] } &<1-10> | **mac-address** *mac-address* } * [ **interface** *interface-type interface-number* ] [ **vlan** *vlan-id* [ **ce-vlan** *ce-vlan-id* ] ] command to configure static binding entries.

After the binding entries are configured, run the **ip source check user-bind enable** command on the specified interface or VLAN. Then unbound hosts cannot go online.

**----End**

# 14.8.6 IPSG Does Not Take Effect When Dynamic IP Address Allocation Is Used Because DHCP Snooping Is Not Configured

## Fault Description

Hosts can obtain IP addresses from the DHCP server, and the IPSG function is enabled; however, IPSG does not take effect.

## Procedure

**Step 1** Check whether the DHCP snooping binding table exists.

When hosts obtain IP addresses through DHCP, IPSG checks packets received by interfaces based on the DHCP snooping dynamic binding table. The device automatically generates DHCP snooping binding entries for online hosts only after the DHCP snooping function is enabled.

**Step 2** Run the **display dhcp snooping user-bind** { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* }* | **all** } command to view DHCP snooping binding entries.

If no dynamic binding entry exists, configure DHCP snooping according to **14.6.2 Configuring IPSG Based on a Dynamic Binding Table**. The major configuration steps are as follows:

1. Enable DHCP snooping globally.
2. Enable DHCP snooping on an interface or in a VLAN.

 Copyright © Huawei Technologies Co., Ltd. 

3. Configure the trusted interface.

After DHCP snooping is configured, the device generates DHCP snooping entries for the hosts when the hosts go online again. Then IPSG takes effect. If you enable IPSG before the device generates DHCP snooping dynamic binding entries, the device rejects all IP packets except DHCP Request packets. In this situation, communication service on the hosts is affected. Therefore, before enabling the IPSG function, configure the DHCP snooping function to enable the device to generate dynamic binding entries.

**----End**

# 14.9 FAQ About IPSG

## 14.9.1 Does a Router Support the Binding of One Interface and Multiple IP Addresses

A router supports the binding of one interface and multiple IP addresses.

- If you need to bind discontinuous IP addresses to an interface, enter 1-10 IP addresses in the command. For example, bind IP addresses 10.1.1.2, 10.1.1.5 and 10.1.1.12 to Eth2/0/0.

  ```
  <Huawei> system-view
  [Huawei] user-bind static ip-address 10.1.1.2 10.1.1.5 10.1.1.12 interface ethernet 2/0/0
  ```

- If you need to bind continuous IP addresses to an interface, enter 1-10 IP address segments in the command. That entered IP address segments cannot overlap. For example, bind IP address segments 10.2.1.1-10.2.1.10 and 10.2.1.20-10.2.1.30 to Eth2/0/0.

  ```
  <Huawei> system-view
  [Huawei] user-bind static ip-address 10.2.1.1 to 10.2.1.10 10.2.1.20 to 10.2.1.30 interface ethernet 2/0/0
  ```

## 14.9.2 Does a Router Support the Binding of One MAC Address and Multiple IP Addresses

A router supports the binding of one MAC address and multiple IP addresses.

- If you need to bind discontinuous IP addresses to a MAC address, enter 1-10 IP addresses in the command. For example, bind IP addresses 10.1.1.2, 10.1.1.5, and 10.1.1.12 to MAC address 0001-0001-0001.

  ```
  <Huawei> system-view
  [Huawei] user-bind static ip-address 10.1.1.2 10.1.1.5 10.1.1.12 mac-address 0001-0001-0001
  ```

- If you need to bind continuous IP addresses to a MAC address, enter 1-10 IP address segments in the command. That entered IP address segments cannot overlap. For example, bind IP address segments 10.2.1.1-10.2.1.10 and 10.2.1.20-10.2.1.30 to MAC address 0002-0002-0002.

  ```
  <Huawei> system-view
  [Huawei] user-bind static ip-address 10.2.1.1 to 10.2.1.10 10.2.1.20 to 10.2.1.30 mac-address 0002-0002-0002
  ```

 Copyright © Huawei Technologies Co., Ltd. 

# 14.9.3 Which Router Models Support IPSG

**Table 14-7** IPSG-capable router models

| Version | Product |
| --- | --- |
| V200R003 and earlier versions | Supported by only the 8FE1GE and 24GE cards of the AR2200&AR3200<br>4GE-2S, 4ES2G-S,4ES2GP-S and 9ES2 cards do not support IPSG.<br>AR150&AR200&AR1200 series do not support IPSG. |
| V200R005C10 and later versions | Supported by all models.<br>Because IPSG supports Layer 2 and Layer 3 traffic monitoring, so AR100&AR120&AR150&AR160&AR200 &AR1200&AR3600 series support only Layer 3 traffic monitoring.<br>**NOTE**<br>4GE-2S, 4ES2G-S, 4ES2GP-S and 9ES2 cards do not support IPSG. |


Copyright © Huawei Technologies Co., Ltd.

# 15 URPF Configuration

## About This Chapter

This chapter describes how to configure URPF to prevent network attacks based on source IP address spoofing.

15.1 Overview of URPF

15.2 Understanding URPF

15.3 Application Scenarios for URPF

15.4 Licensing Requirements and Limitations for URPF

15.5 Default Settings for URPF

15.6 Configuring URPF

15.7 Configuration Examples for URPF

## 15.1 Overview of URPF

### Definition

Unicast Reverse Path Forwarding (URPF) prevents network attacks based on source IP address spoofing.

### Purpose

A Denial of Service (DoS) attack disables users from connecting to the server. DoS attacks aim to occupy excess resources by sending a large number of connection requests. As a result, authorized users cannot receive responses from the server.

URPF searches the outbound interface in the FIB table according to the source IP address of the packet, and checks whether the outbound interface matches the source interface of the packet. If the source IP address does not match the outbound interface of the packet, the packet is discarded. This prevents IP spoofing attacks, especially DoS attacks with bogus source IP address.

 Copyright © Huawei Technologies Co., Ltd. 

### Benefits

- URPF prevents source IP address spoofing attacks and reduces maintenance costs.
- URPF improves network security and stability and defends against malicious attacks.

## 15.2 Understanding URPF

### Working Mode

On a complex network, the routes recorded on the local end and remote end may be different. A URPF-enabled device on this network may discard the packets transmitted along the correct path, but forward the invalid packets.

The device provides the following URPF modes to solve the preceding problem:

- Strict check

  In strict mode, a packet passes the check only when the source IP address of the packet exists in the FIB table and the interface of the default route matches the inbound interface of the packet.

  If route symmetry is ensured, you are advised to use the URPF strict check. For example, if there is only one path between two network edge devices, URPF strict check can be used to ensure network security.
- Loose check

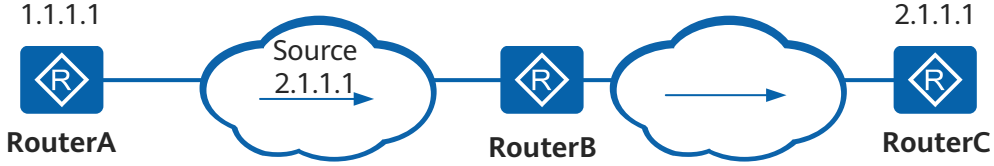
  In loose mode, a packet passes the check as long as the source IP address of the packet matches an entry in the FIB table.

  If route symmetry is not ensured, you are advised to use the URPF loose check. For example, if there are multiple paths between two network edge devices, URPF loose check can be used to ensure network security.

### Working Mechanism

URPF enables the device to search for the source IP address of a received packet in the FIB table to obtain the matching inbound interface. If this inbound interface is different from the inbound interface of the packet, the device considers the source address as a spoofing one and discards the packet. In this manner, URPF can effectively protect the device against malicious attacks by modifying source IP addresses in packets.

**Figure 15-1** URPF working mechanism




As shown in **Figure 15-1**, a bogus packet with source IP address 2.1.1.1 is sent from RouterA to RouterB. After receiving the bogus packet, RouterB sends a

 Copyright © Huawei Technologies Co., Ltd. 

response packet to the actual destination device RouterC at 2.1.1.1. RouterB and RouterC are attacked by the bogus packets.

When RouterB with URPF strict check enabled receives the bogus packet with source IP address 2.1.1.1, URPF discards the packet because the inbound interface of the source IP address is not the interface that receives the packet.

# 15.3 Application Scenarios for URPF

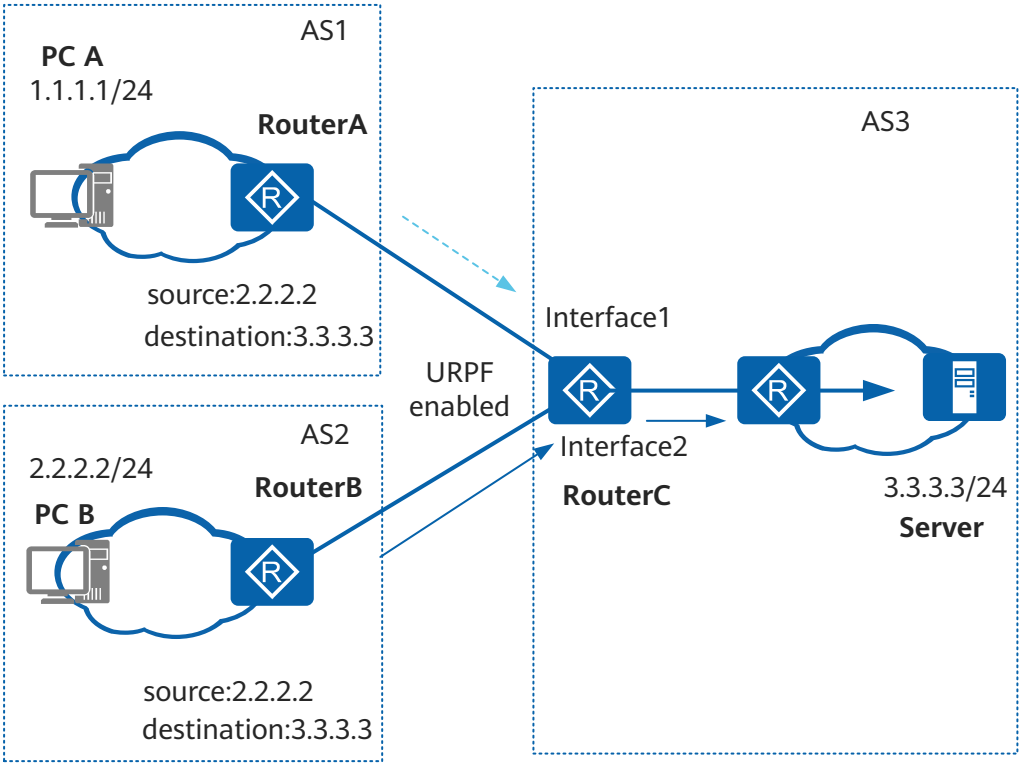
## URPF Strict Check

As shown in **Figure 15-2**, AS1, AS2, and AS3 are unidirectionally connected. URPF is enabled on Interface1 and Interface2 of SwitchC to protect AS3 from source address spoofing attacks from AS1 and AS2.

Assumes that PC A in AS1 generates a packet with the bogus source IP address 2.2.2.2 and sends the packet to the server in AS3. After receiving the packet, RouterC checks the inbound interface of the packet and finds that the packet with the destination IP address 2.2.2.2 must reach RouterC through Interface2. RouterC considers the packet as a bogus packet and discards it.

The packet sent from AS2 to the server is forwarded after passing URPF check.

**Figure 15-2** URPF strict check application



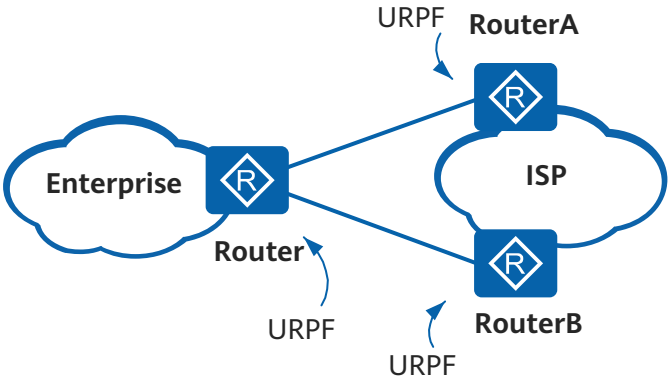

 Copyright © Huawei Technologies Co., Ltd. 

## URPF Loose Check

URPF is often used when multiples connections are set up between two network edge devices.

- Single-homed client connected to one ISP

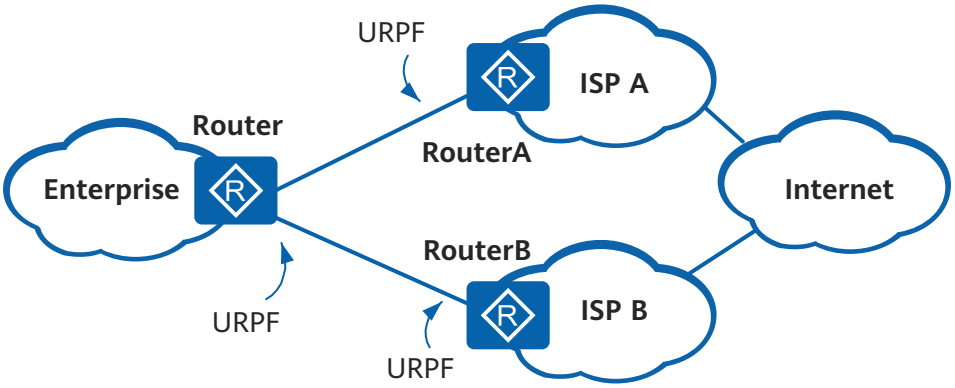
  **Figure 15-3** URPF enabled on single-homed client connected to one ISP




  As shown in **Figure 15-3**, two connections are set up between the enterprise and the ISP device to ensure reliability. In this case, route symmetry between the enterprise and the ISP device cannot be ensured. Therefore, URPF loose check is used.

- Multi-homed client connected to several ISPs

  **Figure 15-4** URPF enabled on multi-homed client connected to several ISPs




  As shown in **Figure 15-4**, the enterprise is connected to several ISPs. Route symmetry between the enterprise and the two ISP devices cannot be ensured. Therefore, URPF loose check is used.

  URPF enabled on multi-homed client connected to several ISPs can be applied to the following situations:

  – If specified packets are required to pass the URPF check in any situations, you can create an ACL to permit packets with specified source IP addresses to pass through.

 Copyright © Huawei Technologies Co., Ltd. 

– The devices connected to users may only have a default route to the ISP. Therefore, matching the default routing entry needs to be supported.

# 15.4 Licensing Requirements and Limitations for URPF

## Involved Network Elements

Other network elements are not required.

## Licensing Requirements

URPF is a basic feature of the router and is not under license control.

## Feature Limitations

None

# 15.5 Default Settings for URPF

Table 15-1 lists the default settings for URPF. The default settings can be modified as required.

**Table 15-1** Default settings for URPF

| Parameter | Default Setting |
| --- | --- |
| URPF check | Disabled |

# 15.6 Configuring URPF

## Pre-configuration Tasks

Before configuring URPF, configure link layer protocol parameters for interfaces to ensure that the link layer protocol status on the interfaces is Up.

# 15.6.1 Configuring the URPF Check Mode on an Interface

## Context

In a complicated networking environment, On a complex network, asymmetric routes may exist. That is, the routes recorded on the local end and remote end are different. A URPF-enabled device on this network may discard the packets transmitted along the correct path, but forward the invalid packets.

The device provides the following URPF modes to solve the preceding problem:

 Copyright © Huawei Technologies Co., Ltd. 

- Strict check

  In strict mode, a packet can pass the check only when the source IP address of the packet exists in the Forwarding Information Base (FIB) table and the related entries and interfaces match.

  If route symmetry is ensured, you are advised to use the URPF strict check. For example, if there is only one path between two network edge devices, URPF strict check can be used to ensure network security.

- Loose check

  In loose mode, the device does not check whether the interfaces of packets exist in the FIB table. A packet can pass the check as long as the source IP address of the packet exists in the FIB table.

  If route symmetry is not ensured, you are advised to use the URPF loose check. For example, if there are multiple paths between two network edge devices, URPF loose check can be used to ensure network security.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface** *interface-type interface-number*

The interface view is displayed.

**Step 3** Configuring URPF check for packets on the interface

- Configure the URPF check mode for IPv4 packets on the interface.

  Run **urpf** { **loose** | **strict** } [ **allow-default-route** ] [ **acl** *acl-number* ]

  The URPF check mode for IPv4 packets is configured on the interface.

- Configure the URPF check mode for IPv6 packets on the interface.

  Run **ipv6 urpf** { **loose** | **strict** } [ **allow-default-route** ] [ **acl** *acl-number* ]

  The URPF check mode for IPv6 packets is configured on the interface.

  NOTE

  To configure URPF check for IPv6 packets on an interface, enable the IPv6 function on the interface first. Run the **ipv6** command in the system view, and run the **ipv6 enable** command in the interface view.

**----End**

# 15.6.2 Verifying the URPF Configuration

## Procedure

**Step 1** Run the **display this** command in the interface view to check whether URPF is enabled on the interface.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

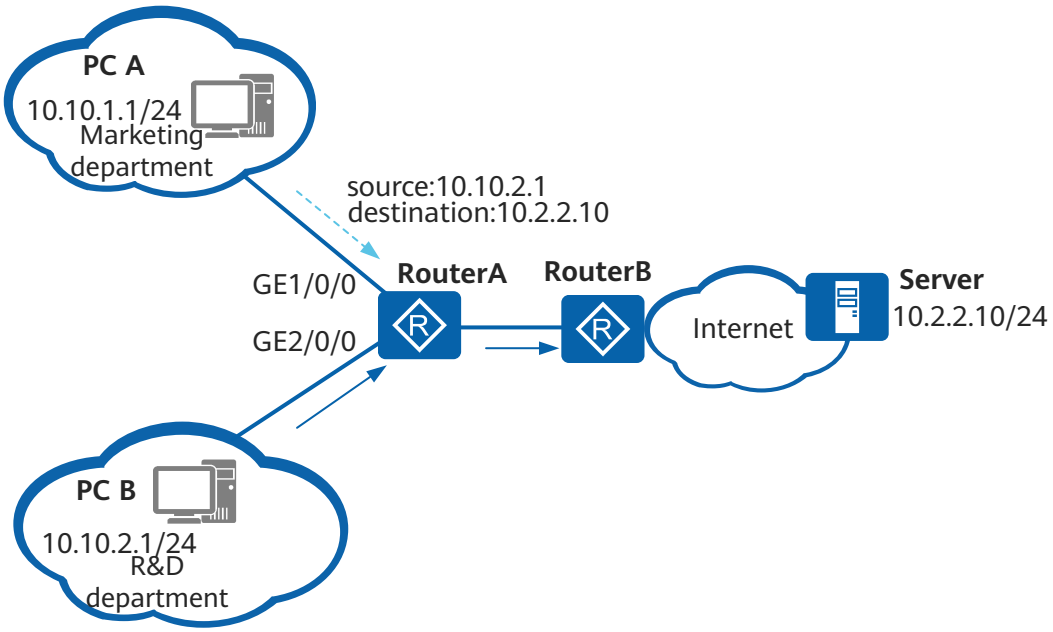
# 15.7 Configuration Examples for URPF

## 15.7.1 Example for Configuring URPF

### Networking Requirements

As shown in **Figure 15-5**, the R&D department of an enterprise connects to GE2/0/0 of RouterA, and the marketing department connects to GE1/0/0. RouterA has a reachable route to an external server, and users in the R&D and marketing departments are allowed to connect to the server through RouterA. RouterA is required to prevent staff in other departments from accessing the server without permission using source IP address spoofing.

**Figure 15-5** Networking diagram of URPF configuration




### Configuration Roadmap

The configuration roadmap is as follows:

Configure URPF on GE1/0/0 and GE2/0/0, and allow special processing for the default route.


Copyright © Huawei Technologies Co., Ltd.

## Procedure

**Step 1** Configure URPF on the interface.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] urpf strict allow-default-route
[RouterA-GigabitEthernet1/0/0] ip address 10.10.1.5 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] ip address 10.10.2.5 24
[RouterA-GigabitEthernet2/0/0] urpf strict allow-default-route
```

**Step 2** Verify the configuration.

# Run the **display this** command on GE1/0/0 to check the URPF configuration.

```
[RouterA-gigabitethernet1/0/0] display this
#
interface GigabitEthernet1/0/0
 ip address 10.10.1.5 255.255.255.0
 urpf strict allow-default-route
#
return
```

# Run the **display this** command on GE2/0/0 to check the URPF configuration.

```
[RouterA-gigabitethernet2/0/0] display this
#
interface GigabitEthernet2/0/0
 ip address 10.10.2.5 255.255.255.0
 urpf strict allow-default-route
#
return
```

**----End**

## Configuration Files

Configuration files on RouterA

```
#
sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.10.1.5 255.255.255.0
 urpf strict allow-default-route
#
interface GigabitEthernet2/0/0
 ip address 10.10.2.5 255.255.255.0
 urpf strict allow-default-route
#
return
```

 Copyright © Huawei Technologies Co., Ltd. 

# 16 PKI Configuration

## About This Chapter

16.1 Overview of PKI
16.2 Understanding PKI
16.3 Application Scenarios for PKI
16.4 Licensing Requirements and Limitations for PKI
16.5 Default Settings for PKI
16.6 Summary of PKI Configuration Tasks
16.7 Configuring PKI
16.8 Maintaining PKI
16.9 Configuration Examples for PKI
16.10 Troubleshooting PKI
16.11 FAQ About PKI

## 16.1 Overview of PKI

### Definition

Public Key Infrastructure (PKI) provides certificate management in compliance with certain standards. It uses public keys to provide security service for all network applications. PKI is the core of information security and basis of e-commerce.

### Purpose

As the network and information technologies develop, e-commerce is widely used and accepted. However, e-commerce has the following problems:

 Copyright © Huawei Technologies Co., Ltd. 

- The transaction parties cannot verify the identities of each other.
- Data may be eavesdropped and tampered with during transmission. Information is not secure.
- No paper receipt is used in transaction, making arbitration difficult.

PKI uses public keys to implement identity verification, confidentiality, data integrity, and non-repudiation of transactions. Therefore, PKI is widely used in network communication and transactions, especially e-government and e-commerce.

### Benefits

- Benefits to users
  - Certificate authentication allows users to authenticate network devices to which they connect, ensuring that users connect to secure and legal networks.
  - Cryptography protects data against tampering and eavesdropping so that data is securely transmitted.
  - Digital signature ensures that data is accessible to only authorized devices and users, protecting data privacy.
- Benefits to enterprises
  - PKI prevents unauthorized users from connecting to enterprise networks.
  - PKI establishes secure connections between enterprise branches to ensure data security.

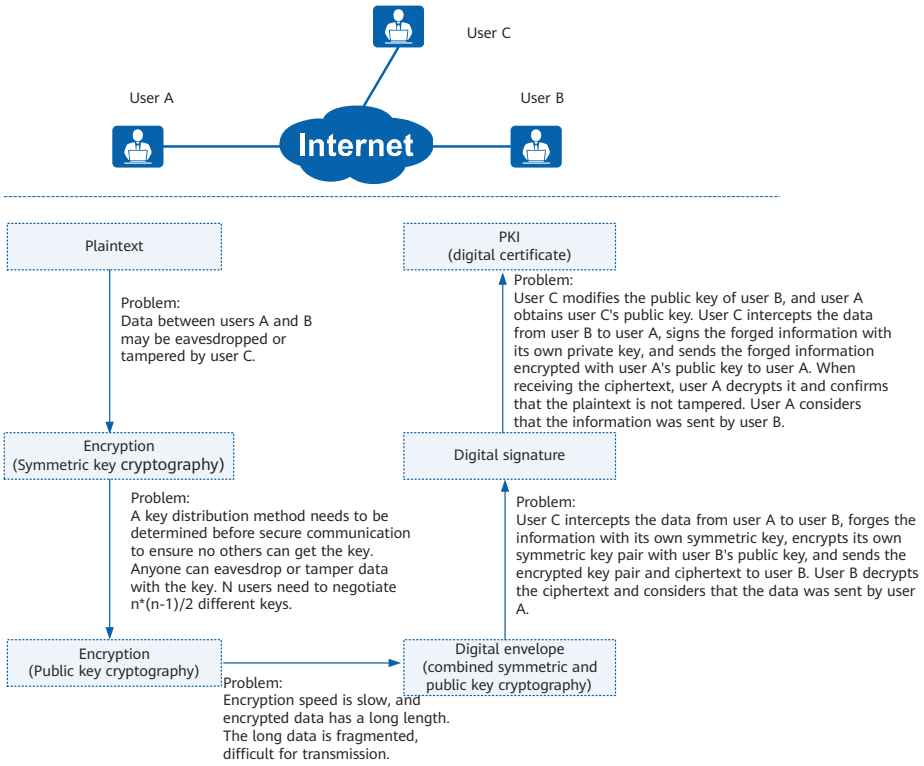
## 16.2 Understanding PKI

### 16.2.1 Basic Concepts of PKI

The core of PKI is digital certificate lifecycle management, including applying for, issuing, and using the digital certificates. During the lifecycle, PKI uses the symmetric key cryptographic, public key cryptographic, digital envelope, and digital signature. **Figure 16-1** shows the evolution of these technologies. Users A and B communicate through the Internet, and user C is the attacker who targets the communication data between users A and B.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 16-1** Technology evolution




The concepts mentioned in the figure will be described in later sections.

## 16.2.1.1 Cryptography

Cryptography is the basis for secure information transmission on networks. Cryptography is to convert plaintext (to be hidden) into ciphertext (unreadable data) using mathematics.

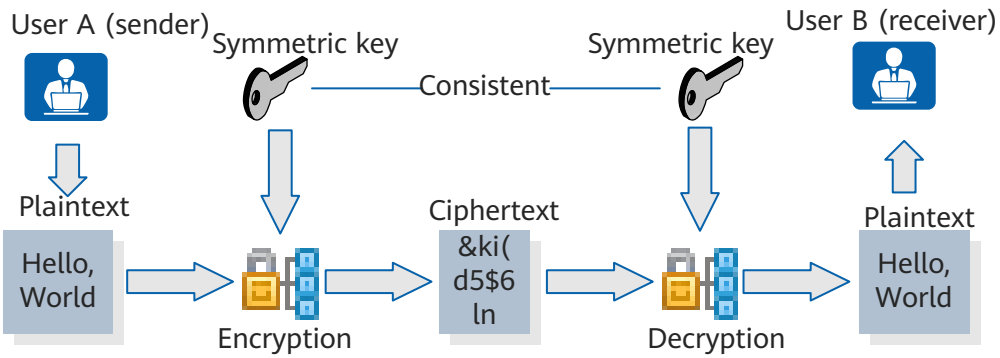
## Symmetric Key Cryptography

Symmetric key cryptography, which is also called shared key cryptography, uses the same key to encrypt and decrypt data.

**Figure 16-2** shows the symmetric key encryption and decryption process.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 16-2** Symmetric key encryption and decryption process




Users A and B have negotiated the symmetric key. The encryption and decryption process is as follows:

1. User A uses the symmetric key to encrypt data and sends the encrypted data to user B.
2. User B decrypts the data using the symmetric key and gets the original data.

Symmetric key cryptography features high efficiency, simple algorithm, and low cost. It is suitable for encrypting a large amount of data. However, it is difficult to implement because the two parties must exchange their keys securely before communication. Besides, it is difficult to expand because each pair of communicating parties needs to negotiate keys, and n users needs to negotiate n*(n-1)/2 different keys.

The algorithms commonly used in symmetric key cryptography include Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), and Advance Encrypt Standard (AES).

## Public Key Cryptography

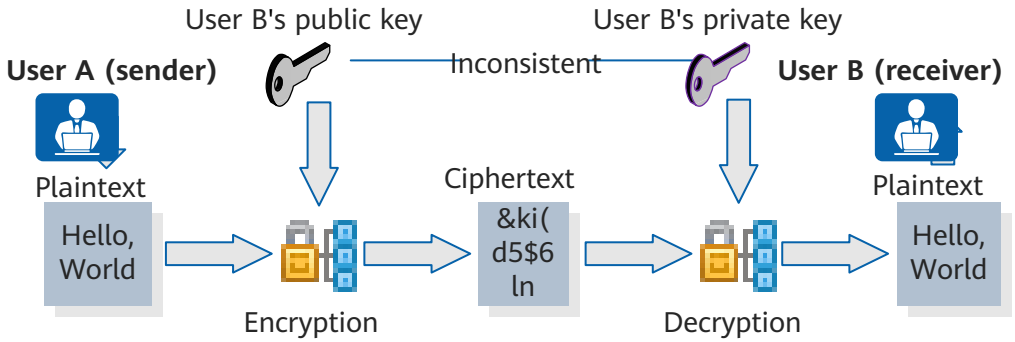
Public key cryptography, which is also called asymmetric key cryptography, uses different keys (public and private) for data encryption and decryption. The public key is open to public, and the private key is possessed by only the owner.

Public key cryptography prevents the security risks in the distribution and management of a symmetric key. In an asymmetric key pair, the public key is used to encrypt data and the private key is used to decrypt data. The two parties do not need to exchange keys before a secure communication session. The sender uses the public key of the receiver to encrypt the data, and the receiver uses its own private key to decrypt data. The receiver's private key is only known by the receiver, so the data is secure.

**Figure 16-3** shows the public key encryption and decryption process.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 16-3** Public key encryption and decryption process




Assume that user A has the public key of user B. The encryption and decryption process is as follows:

1. User A uses the public key of user B to encrypt data and sends the encrypted data to user B.
2. User B decrypts the data using its own private key and gets the original data.

Attackers cannot use one key in a key pair to figure out the other key. The data encrypted by a public key can only be decrypted by the private key of the same user. However, the public key cryptography requires a long time to encrypt a large amount of data, and the encrypted data is too long, consuming much bandwidth.

Public key cryptography is suitable for encrypting sensitive information such as keys and identities to provide higher security.

The algorithms commonly used in public key cryptography include Diffie-Hellman (DH), Ron Rivest, Adi Shamirh, LenAdleman (RSA), and Digital Signature Algorithm (DSA).

## 16.2.1.2 Digital Envelope and Digital Signature

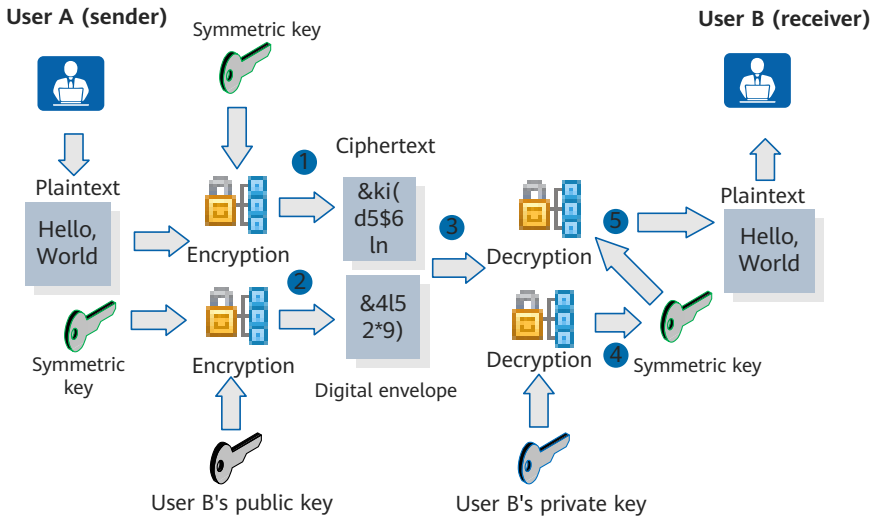
## Digital Envelope

A digital envelope contains the symmetric key encrypted using the peer's public key. When receiving a digital envelope, the receiver uses its own private key to decrypt the digital envelope and obtains the symmetric key.

**Figure 16-4** shows the encryption and decryption process for a digital envelope.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 16-4** Digital envelope encryption and decryption process




Assume that user A has the public key of user B. The encryption and decryption process is as follows:

1. User A uses a symmetric key to encrypt data.
2. User A uses the public key of user B to encrypt the symmetric key and generate a digital envelope.
3. User A sends the digital envelope and encrypted data to user B.
4. User B uses its own private key to decrypt the digital envelope and obtains the symmetric key.
5. User B uses the symmetric key to decrypt the data and obtains the original data.

The digital envelope has the advantages of both symmetric key cryptography and public key cryptography. It speeds up key distribution and encryption and improves key security, extensibility, as well as efficiency.

However, the digital envelope still has a vulnerability. The attacker may obtain information from user A, use its own symmetric key to encrypt the forged information, use the public key of user B to encrypt its own symmetric key, and send the information to user B. After receiving the information, user B decrypts it and considers that the information is sent from user A. To address this problem, the digital signature is used to ensure that the received information was sent from the correct sender.

## Digital Signature

Digital signature is generated by the sender by encrypting the digital fingerprint using its own private key. The receiver uses the sender's public key to decrypt the digital signature and obtain the digital fingerprint.

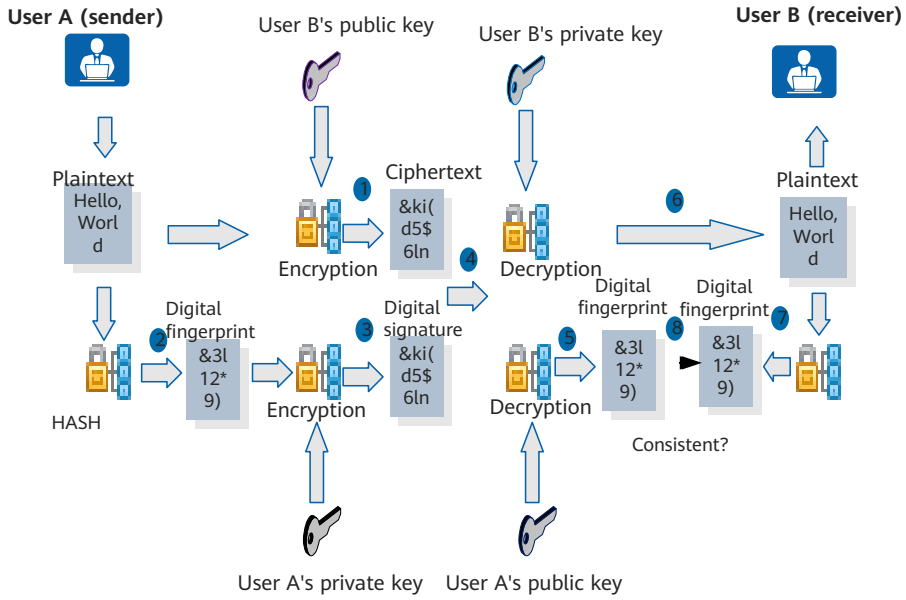
A digital fingerprint, which is also called information digest, is generated by the sender using the hash algorithm on plaintext information. The sender sends both

 Copyright © Huawei Technologies Co., Ltd. 

digital fingerprint and plaintext to the receiver, and the receiver uses the same hash algorithm to calculate the digital fingerprint on the plaintext. If the two fingerprints are the same, the receiver knows that the information has not been tampered with.

**Figure 16-5** shows the encryption and decryption process for a digital signature.

**Figure 16-5** Digital signature encryption and decryption process




Assume that user A has the public key of user B. The encryption and decryption process is as follows:

1. User A uses the public key of user B to encrypt data.
2. User A performs hash on the plaintext and generates a digital fingerprint.
3. User A uses its own private key to encrypt the digital fingerprint, generating the digital signature.
4. User A sends both the ciphertext and digital signature to user B.
5. User B uses the public key of user A to decrypt the digital signature, obtaining the digital fingerprint.
6. After receiving the ciphertext from user A, user B uses its own private key to decrypt the information, obtaining the plaintext information.
7. User B performs hash on the plaintext and generates a digital fingerprint.
8. User B compares the generated fingerprint with the received one. If the two fingerprints are the same, user B accepts the plaintext; otherwise, user B discards it.

The digital signature proves that information is not tampered with and verifies the sender's identity. The digital signature and digital envelope can be used together.

 Copyright © Huawei Technologies Co., Ltd. 

However, the digital signature still has a vulnerability. If the attacker modifies the public key of user B, then user A obtains the attacker's public key. The attacker can obtain information from user B to user A, sign the forged information using its own private key, and send the forged information encrypted using user A's public key to user A. After receiving the encrypted information, user A decrypts the information and verifies that the information has not been tampered with. In addition, user A considers that the information was sent by user B. The digital certificate can fix this vulnerability. It ensures that one public key is possessed by only one owner.

### 16.2.1.3 Digital Certificate

A digital certificate, or certificate, which is signed by the trusted certificate authority (**CA**) using digital signature, includes the certificate owner's public key and identity information.

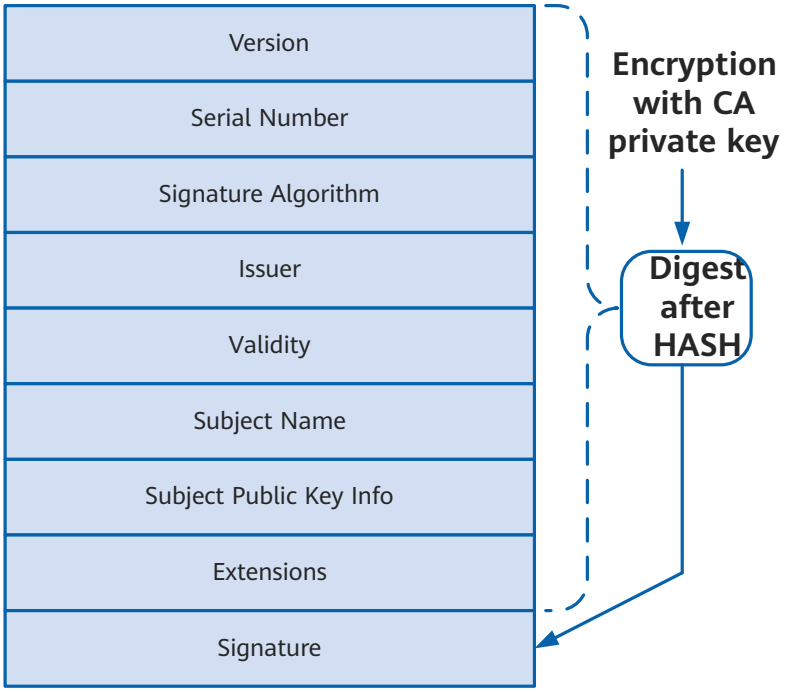
The digital certificate is similar to the passport or identity card. People are requested to show their passports when entering foreign countries. The digital certificate shows the identity of a device or user that requests to access a network.

It ensures that one public key is possessed by only one owner.

### Digital Certificate Structure

An X.509 v3 digital certificate contains mandatory information such as public key, name, and digital signature of the CA, and optional information such as validity period of the key, issuer (CA) name, and serial number. **Figure 16-6** shows the typical structure of a digital certificate.

**Figure 16-6** Digital certificate structure diagram





Copyright © Huawei Technologies Co., Ltd.

Meaning of each field in the digital certificate:

- Version: version of X.509. Generally, the v3 (0x2) is used.
- Serial Number: a positive and unique integer assigned by the issuer to the certificate. Each certificate is uniquely identified by the issuer name and the serial number.
- Signature Algorithm ID: signature algorithm used by the issuer to sign the certificate.
- Issuer: name of the device that has issued a certificate. It must be the same as the subject name in the digital certificate. Generally, the issuer name is the CA server's name.
- Validity: time interval during which a digital certificate is valid, including the start and end dates. The expired certificates are invalid.
- Subject: name of the entity that possesses a digital certificate. In a self-signed certificate, the issuer name is the same as the subject name.
- Subject Public Key Info: public key and the algorithm with which the key is generated.
- Extensions: a sequence of optional fields such as key usage and CRL distributing address.
- Signature: signature signed on a digital certificate by the issuer using the private key.

## Digital Certificate Types

There are four types of certificates, as described in **Table 16-1**.

**Table 16-1** Certificate types

| Type | Definition | Description |
| --- | --- | --- |
| Self-signed certificate | A self-signed certificate, which is also called root certificate, is issued by an entity to itself. In this certificate, the issuer name and subject name are the same. | If an applicant fails to apply for a local certificate from the CA, it can generate a self-signed certificate. The self-signed certificate issuing process is simple.<br>A device does not support lifecycle management (such as certificate update and revocation) over its self-signed certificate. To ensure security of the device and certificate, you are advised to replace the self-signed certificate with the local certificate. |

 Copyright © Huawei Technologies Co., Ltd. 

| Type | Definition | Description |
| --- | --- | --- |
| CA certificate | CA's own certificate. If a PKI system does not have a hierarchical CA structure, the CA certificate is the self-signed certificate. If a PKI system has a hierarchical CA structure, the top CA is the root CA, which owns a self-signed certificate. | An applicant trusts a CA by verifying its digital signature. Any applicant can obtain the CA's certificate (including the public key) to verify the local certificate issued by the CA. |
| Local certificate | A certificate issued by a CA to the applicant. | - |
| Local device certificate | A certificate issued by a device to itself according to the certificate issued by the CA. The issuer name in the certificate is the CA server's name. | If an applicant fails to apply for a local certificate from the CA, it can generate a local device certificate. The local device certificate issuing process is simple. |

## Certificate Formats

Three certificate formats are supported, as described in **Table 16-2**.

**Table 16-2** Certificate formats

| Format | Description | Description |
| --- | --- | --- |
| PKCS#12 | Saves certificate files in binary format, including or excluding the private key. The commonly used file name extensions include .P12 and .PFX. | If the file name extension of a certificate is .CER or .CRT, use the Notepad to open this certificate and check the certificate content to differentiate the certificate format.<br>• If the certificate starts with "-----BEGIN CERTIFICATE-----" and ends with "-----END CERTIFICATE-----", the certificate format is PEM. |
| DER | Saves certificate files in binary format, excluding the private key. The commonly used file name extensions include .DER, .CER, and .CRT. | |

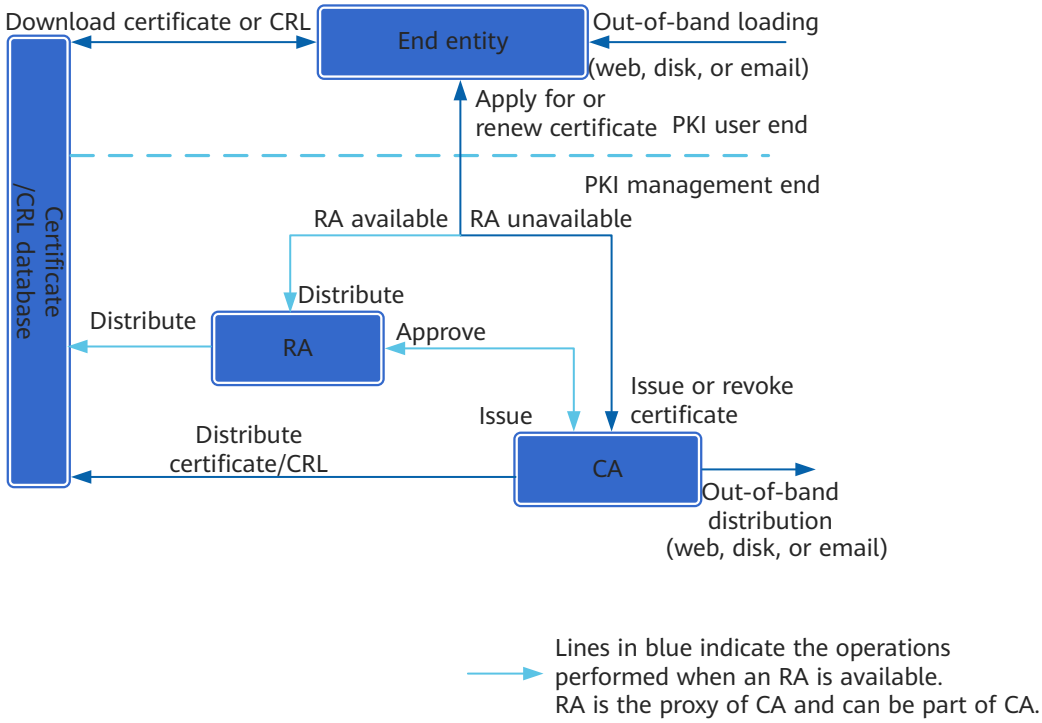
 Copyright © Huawei Technologies Co., Ltd. 

| Format | Description | Description |
| --- | --- | --- |
| PEM | Saves certificate files in ASCII format, including or excluding the private key. The commonly used file name extensions include .PEM, .CER, and .CRT. | • If the certificate content is displayed as garbled characters, the certificate format is DER. |

## 16.2.2 PKI System Structure

As shown in **Figure 16-7**, a PKI system consists of the end entity, certificate authority (CA), registration authority (RA), and certificate/certificate revocation list (CRL) storage database.

**Figure 16-7** PKI system structure




- End entity

  An end entity, or PKI entity, is the end user of PKI products or services. It can be an individual, an organization, a device (for example, a router or firewall), or process running on a computer.

- Certificate Authority (CA)

  The CA is the trusted entity that issues and manages digital certificates. The CA is an authoritative, trustable, and fair third-party organization. Generally, a CA is a server, for example, a server running Windows Server 2008.

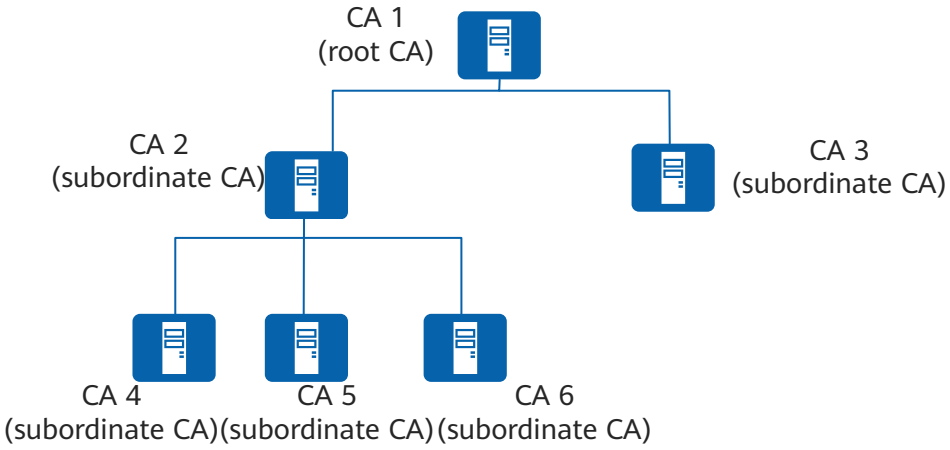
 Copyright © Huawei Technologies Co., Ltd. 

Figure 16-8 shows a hierarchical CA. The CA on the top of the hierarchy is the root CA and the others are subordinate CAs.

- The root CA is the first CA (trustpoint) in the PKI system. It issues certificates to subordinate CAs, computers, users, and services. In most certificate-based applications, the root CA can be traced through the certificate chain. The root CA holds a self-signed certificate.
- A subordinate CA can only obtain a certificate from its upper-level CA. The upper-level CA can be the root CA or another subordinate CA authorized by the root CA to issue certificates. The upper-level CA is responsible issuing and managing certificates of lower-level CAs, and the CAs at the bottom issue certificates to end entities. For example, CA 2 and CA 3 are subordinate CAs, holding the certificates issued by CA 1, and CA 4, CA 5, as well as CA 6 are also subordinate CAs, holding the certificates issued by CA 2.

When a PKI entity trusts a CA, the trust is derived along the certificate chain. A certificate chain is a set of certificates from the end entity to the root certificate. When a PKI entity in communication receives a certificate to be authenticated, the PKI entity verifies each issuer along the certificate chain.

**Figure 16-8** Hierarchical CA diagram




Certificate management is the major function of CAs, including issuing, renewing, revoking, querying, and archiving certificates as well as distributing the Certificate Revocation List (CRL).

- Registration Authority (RA)

  An RA enrolls and approves digital certificates. It is a proxy for the CA and provides extended applications of certificate issuing and management. The RA processes the certification enrollment and revocation requests from users, verifies user identities, and decides whether to submit certificate issuing or revocation requests to the CA.

  The RA may be part of the CA server, or independent of CA to share workload of CA and enhance CA system security.

- Certificate/CRL database

  A certificate may need to be revoked for the reasons such as entity name changing, private key leaking, or service interruption. Revoking a certificate is

 Copyright © Huawei Technologies Co., Ltd. 

to unbind the public key from the PKI entity identity information. The PKI system uses a CRL to revoke certificates.

After a certificate is revoked, the CA issues a CRL to declare that the certificate is invalid and lists the serial numbers of revoked certificates. The CRL provides a method to verify certificate validity.

The certificate/CRL database stores and manages information about certificates and CRLs and allows information query. The certificate/CRL database can be built using a Lightweight Directory Access Protocol (LDAP) server, File Transfer Protocol (FTP) server, Hypertext Transfer Protocol (HTTP) server, or database. LDAP simplifies the directory access protocol X.500. It supports TCP/IP and has been widely used in certificate distribution, CRL distribution, CA policies, and information distribution. If the number of certificates is small, the certificates can be stored on an HTTP or FTP server and are allowed to be downloaded.

PKI manages the entire lifecycle of local certificates, including application, issue, storage, download, installation, authentication, renewal, and revocation.

## Certificate Application

Certificate application is certificate enrollment. It is a process in which an entity registers with a CA and obtains a certificate from the CA. Generally, a PKI entity generates a pair of public and private keys. The public key and entity's identity information (included in certificate enrollment request) are sent to the CA to generate a local certificate. The private key is stored by the PKI entity to perform digital signature and decrypt the ciphertext sent from the peer.

A PKI entity can use either of the following methods to apply for a local certificate from CA:

- Online

  The PKI entity sends certificate enrollment requests to the CA by using the Simple Certificate Enrollment Protocol (SCEP) or Certificate Management Protocol version 2 (CMPv2).
- Offline (PKCS#10)

  The PKI entity prints the local certificate enrollment request in PKCS#10 format and saves it as a file. Then the user transfers the file to the CA server in out-of-band mode (web, disk, or email).

In addition, a PKI entity can issue a self-signed or local certificate to itself.

## Certificate Issue

If an RA is available, the RA verifies the PKI entity's identity information when the PKI entity applies for a local certificate from CA. After the PKI entity passes verification, the RA sends the request to CA. The CA generates a local certificate based on the public key and identity information of the PKI entity, and then returns the local certificate information to the RA. If no RA is available, the CA verifies the PKI entity.

 Copyright © Huawei Technologies Co., Ltd. 

## Certificate Storage

After the CA generates a local certificate, the CA or RA distributes the certificate to the certificate/CRL database. Users can download or browse directory of the certificates in the database.

## Certificate Downloading

A PKI entity can download a local certificate, a CA/RA certificate, or a local certificate of another PKI entity from the CA server using SCEP, CMPv2, LDAP, HTTP, or out-of-band mode.

## Certificate Installation

A downloaded certificate (a local certificate, CA/RA certificate, or certificate of another PKI entity) must be installed on the device, that is, imported to the device memory; otherwise, the certificate does not take effect.

## Certificate Authentication

Before a PKI entity uses a certificate obtained from the peer, for example, for the purposes of setting up a security tunnel or connection, the PKI entity authenticates the certificate and CA (whether the certificate is valid and issued by the expected CA). If the certificate is invalid, the PKI considers all certificates issued by this CA invalid. This seldom occurs because a device renews the CA certificate before expiration in normal situations.

The PKI entity uses CRL or Online Certificate Status Protocol (OCSP) to authenticate certificates. In CRL mode, the PKI entity searches for the certificate in the CRL stored in local memory. If the certificate is included in the CRL, it indicates that the certificate has been revoked. If no CRL is available in local memory, a CRL needs to be downloaded and installed. In OCSP mode, the PKI entity sends a certificate status query message to the OCSP server, and the OCSP server returns the certificate state, including valid (not revoked), expired (revoked), and unknown (OCSP server cannot find the certificate status).

## Certificate Renewal

When a certificate expires or the private key is leaked, the PKI entity must replace the certificate. The PKI entity can apply for a new certificate or use SCEP or CMPv2 to renew the existing certificate.

When a certificate is about to expire, the device applies for a shadow certificate. When the certificate expires, the shadow certificate becomes active.

The shadow certificate application process is the enrollment process for the new certificate.

## Certificate Revocation

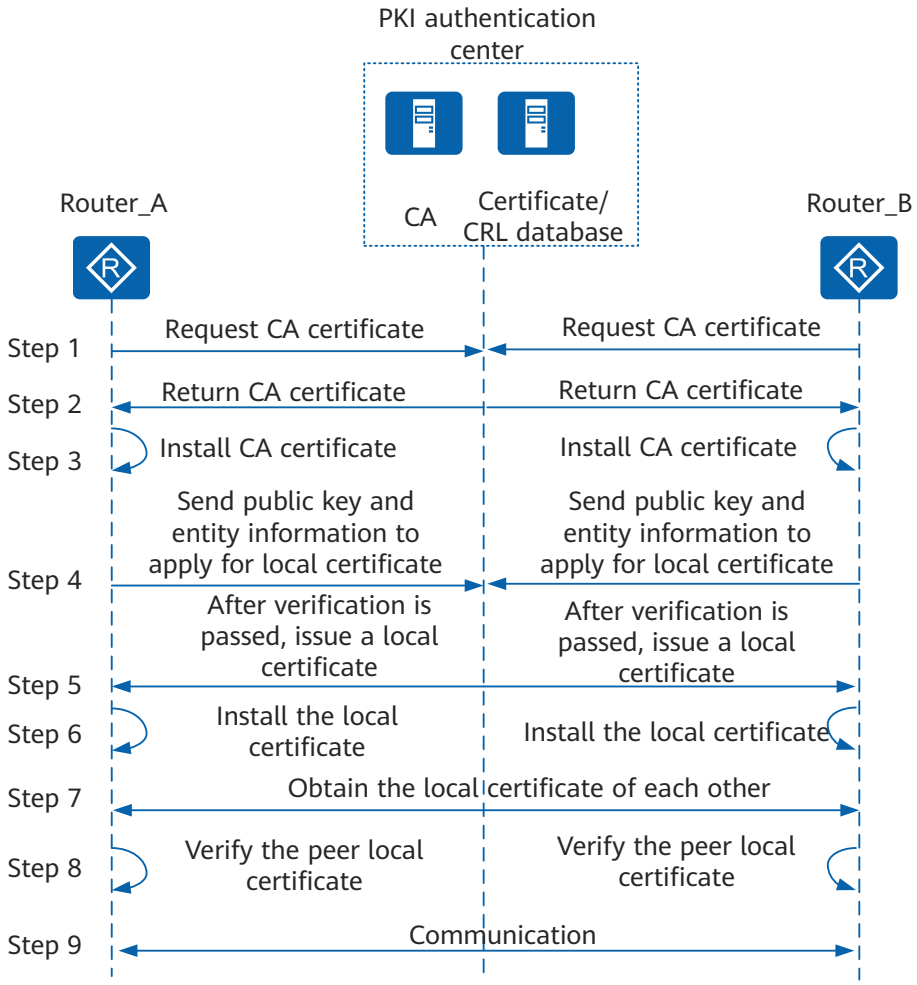
When the user identity, user information, or public key is modified or user service needs to be interrupted, a certificate revocation is required. Certificate revocation unbinds a public key from the PKI entity's identity information. The CA uses CRL or OCSPto revoke certificates for PKI entities, whereas a PKI entity revokes its own certificate in out-of-band mode.

 Copyright © Huawei Technologies Co., Ltd. 

## 16.2.3 PKI Working Mechanism

On a PKI network, a PKI entity applies for a local certificate from the CA and the applicant device authenticates the certificate. **Figure 16-9** shows the PKI working process.

**Figure 16-9** PKI working process




1. A PKI entity applies for a CA certificate (CA server's certificate) from the CA.
2. When receiving the application request, the CA sends its own certificate to the PKI entity.
3. The PKI entity installs the CA certificate.

   If the PKI entity uses SCEP for certificate application, it computes a digital fingerprint by using the hash algorithm on the received CA certificate, and compares the computed fingerprint with that pre-defined for the CA server. If the fingerprints are the same, the PKI accepts the CA certificate; otherwise, it discards the CA certificate.


Copyright © Huawei Technologies Co., Ltd.

4. The PKI entity sends a certificate enrollment message (including the public key carried in the configured key pair and PKI entity information) to the CA.
   - If the PKI entity uses SCEP for certificate application, it encrypts the enrollment message using the CA certificate's public key and signs the message using its own private key. If the CA server requires a challenge password, the enrollment message must contain a challenge password, which must be the same as the CA's challenge password.
   - If the PKI entity uses CMPv2 to apply for a local certificate, it uses an external identity certificate (local certificate issued by another CA) or MAC to authenticate the certificate.
     - External identity certificate

       The PKI entity uses the CA certificate's public key to encrypt the enrollment message and the external identity certificate's private key for digital signature.
     - MAC

       The PKI entity uses the CA certificate's public key to encrypt the enrollment message and the message must contain the MAC reference value and secret value (the values must be the same as those of the CA).
5. The CA receives the enrollment message from the PKI entity.
   - If the PKI entity uses SCEP to apply for a local certificate, the CA uses its own private key to decrypt the enrollment message and the PKI entity's public key to decrypt the digital signature, and verifies the digital fingerprint. When the fingerprints are the same, the CA verifies the PKI entity's identity information. When the PKI entity's identity information passes verification, the CA accepts the application and issues a local certificate to the PKI entity. The CA uses the PKI entity's public key to encrypt the certificate and its own private key to digitally sign the certificate, and sends the certificate to the PKI entity. At the same time, the CA also sends the certificate to the certificate/CRL database.
   - If the PKI entity uses CMPv2 to apply for a local certificate, the CA can use two modes:
     - External identity certificate

       The CA uses its own private key to decrypt the enrollment message and external identity certificate's public key to decrypt the digital signature, and verifies the digital fingerprint. When the fingerprints are the same, the CA verifies the PKI entity's identity information. When the PKI entity's identity information passes verification, the CA accepts the application and issues a local certificate to the PKI entity. The CA uses the public key in the PKI entity's external identity certificate to encrypt the certificate and its own private key to digitally sign the certificate, and sends the certificate to the PKI entity. At the same time, the CA also sends the certificate to the certificate/CRL database.
     - MAC

       The CA uses its own private key to decrypt the enrollment message and verifies the MAC reference value and secret value. When the reference value and secret value are the same as those on the CA

 Copyright © Huawei Technologies Co., Ltd. 

server, the CA verifies the PKI entity's identity information. When the PKI entity's identity information passes verification, the CA accepts the application and issues a local certificate to the PKI entity. The CA then uses the PKI entity's public key to encrypt the certificate, and issues the certificate to the PKI entity. At the same time, the CA also sends the certificate to the certificate/CRL database.

6. The PKI entity receives the certificate from CA.
   - If the PKI entity has applied for a local certificate using SCEP, the PKI entity uses its own private key to decrypt the certificate and the CA's public key to decrypt the digital signature, and verifies the digital fingerprint. If the digital fingerprint is the same as its local one, the PKI entity accepts and installs the local certificate.
   - If the PKI entity has applied for a local certificate using CMPv2:
     - External identity certificate

       The PKI entity uses the external identity certificate's private key to decrypt the certificate and the CA's public key to decrypt the digital signature, and verifies the digital fingerprint. If the digital fingerprint is the same as its local one, the PKI entity accepts and installs the local certificate.
     - MAC

       The PKI entity uses its own private key to decrypt the certificate and verifies the MAC reference value and secret value. If the reference value and secret value are the same as the local ones, the PKI entity accepts and installs the local certificate.
7. The PKI entities in a communication session need to obtain and install each other's local certificates. The PKI entities can download the peer's local certificates through HTTP or LDAP.
8. After the peer's local certificate is installed on the local end, the local end uses CRL or OCSP to check whether the peer certificate is valid.
9. The PKI entities use the public keys in peer certificates for secure communication only after they confirm that the peer certificates are valid.

If an RA is available in a PKI system, the PKI entities also need to download the RA's certificate. The RA verifies the local certificate enrollment messages from PKI entities, and forwards the messages to the CA after verifications are passed.

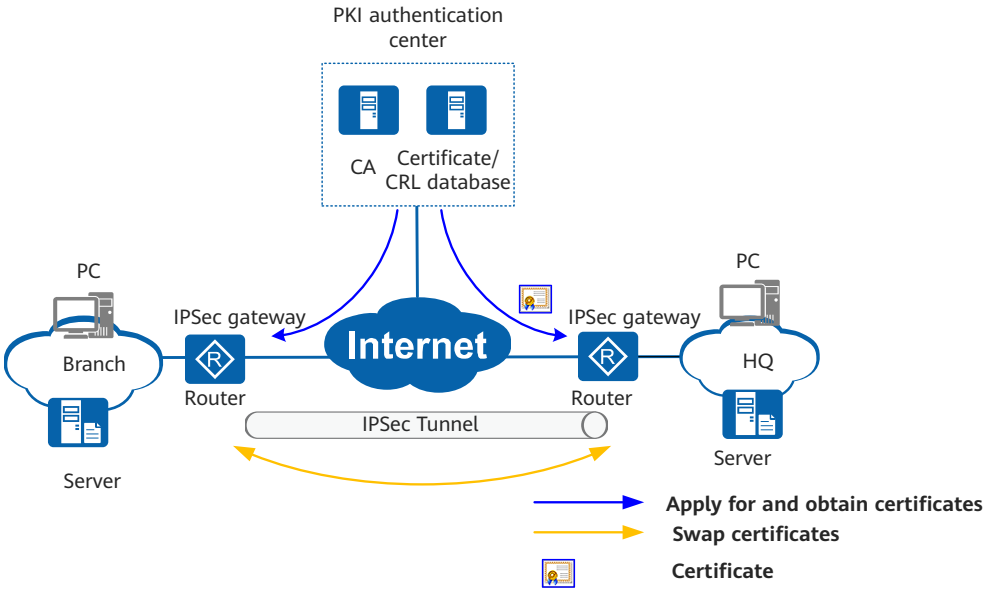
# 16.3 Application Scenarios for PKI

## 16.3.1 PKI Application in IPSec VPN

On the network shown in **Figure 16-10**, the firewalls function as egress gateways of network A and network B. The internal users of the two networks communicate through the Internet. To ensure data security over the Internet, the firewalls have IPSec configured to set up an IPSec tunnel. Generally, IPSec can use pre-shared key to negotiate the IPSec tunnel. However, using a pre-shared key on a large network is not security and time consuming. To address this problem, the devices can use PKI certificates to authenticate each other in PKI tunnel setup.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 16-10** PKI application in IPSec VPN




After PKI is configured, communicating parties authenticate each other during IKE negotiation. This ensures security in key exchange. In addition, the certificate provides a centralized key management function for IPSec and enhances scalability of the entire IPSec network. On an IPSec network with PKI configured, each device has a locate certificate issued by the PKI authentication center. When a new device is deployed, the new device can securely communicate with other devices by applying for a certificate, and the configurations on other devices do not need to be modified. This greatly reduces configuration workload.

# 16.4 Licensing Requirements and Limitations for PKI

## Involved Network Elements

- PKI authentication center (including CA server, certificate/CRL storage server, and so on)
- PKI entity

## Licensing Requirements

The PKI function is not under license control.

## Feature Limitations

None.

 Copyright © Huawei Technologies Co., Ltd. 

# 16.5 Default Settings for PKI

**Table 16-3** Default settings for PKI

| Parameter | Default Setting |
| --- | --- |
| PKI entity | None |
| PKI realm | default |
| RSA key pair | default |
| SM2 key pair | None |
| Format of saved certificate request, certificate, and CRL | PEM |
| Certificate check method | CRL |

# 16.6 Summary of PKI Configuration Tasks

**Table 16-4** describes the PKI configuration tasks.


Copyright © Huawei Technologies Co., Ltd.

**Table 16-4** PKI configuration tasks

| Scenario | Description | Task |
| --- | --- | --- |
| Apply for the local certificate online. | You can use SCEP or CMPv2 to apply for the local certificate online. Both SCEP and CMPv2 can be used for automatic certificate update. SCEP is easier to maintain than CMPv2, but CMPv2 can be used to apply for a local certificate for another device. | When using SCEP to apply for the local certificate, perform the operations in the following order:<br>1. **16.7.1 Preconfiguring a Local Certificate**<br>2. **16.7.2.1 Applying for and Updating the Local Certificate Through SCEP** in **16.7.2 Applying for and Updating Local Certificate**<br>3. **16.7.5 Verifying the CA and Local Certificates**<br>When using CMPv2 to apply for the local certificate, perform the following operations in order:<br>1. **16.7.1 Preconfiguring a Local Certificate**<br>2. **16.7.2.2 Applying for and Updating the Local Certificate Through CMPv2** in **16.7.2 Applying for and Updating Local Certificate**<br>3. **16.7.4 (Optional) Installing the Local Certificate**<br>4. **16.7.5 Verifying the CA and Local Certificates** |


Copyright © Huawei Technologies Co., Ltd.

| Scenario | Description | Task |
| --- | --- | --- |
| Apply for the local certificate offline. | This is the only choice used when the device is unable to access the CA server due to some reasons such as network inaccessible.<br>You can generate the certificate application file on the device, and transfer the file to the CA to apply for a license in out of band mode (for example, web, disk, and email). Alternatively, you can directly send the certificate application information to the CA through web. | When you generate the certificate application file on the device, perform the following operations in order:<br>1. **16.7.1 Preconfiguring a Local Certificate**<br>2. **16.7.2.3 Applying for the Local Certificate in Offline Mode** in **16.7.2 Applying for and Updating Local Certificate**<br>3. **16.7.3 (Optional) Downloading a Local Certificate**<br>4. **16.7.4 (Optional) Installing the Local Certificate**<br>5. **16.7.5 Verifying the CA and Local Certificates**<br>When you send the certificate application information to the CA through web, perform the following operations in order:<br>1. Send certificate application information to the CA through web.<br>2. Download the CA certificate, local certificate, and key pair, and upload them to the storage media.<br>3. Install the key pair. For details, see **16.7.1.2 Configuring an RSA Key Pair** in **16.7.1 Preconfiguring a Local Certificate**.<br>4. Install the CA certificate. For details, see **16.7.1.3.2 (Optional) Installing a CA Certificate for a PKI Entity** in **16.7.1 Preconfiguring a Local Certificate**.<br>5. Install the local certificate. For details, see **16.7.4** |

 Copyright © Huawei Technologies Co., Ltd. 

| Scenario | Description | Task |
| --- | --- | --- |
| | | **(Optional) Installing the Local Certificate**.<br>6. Verify the certificates. For details, see **16.7.5 Verifying the CA and Local Certificates**. |

# 16.7 Configuring PKI

## 16.7.1 Preconfiguring a Local Certificate

### 16.7.1.1 Configuring a PKI Entity

#### Context

Local certificates are signed and issued by the CA. A local certificate is a bundle of public key and PKI entity. PKI entity information contains the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. Therefore, the PKI entity must send the certificate enrollment request carrying PKI entity information to the CA when applying for a local certificate.

#### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **pki entity** *entity-name*

A PKI entity is created and the PKI entity view is displayed; or the PKI entity view is displayed directly.

By default, no PKI entity is configured.

NOTE

Windows Server 2003 has a low processing performance. When the device is connected to a Windows Server 2003, the device cannot have too many entities configure or use the key pair with a large size. Otherwise, the device may fail to connect to the server.

**Step 3** Run **common-name** *common-name*

A common name is configured for the PKI entity.

By default, no common name is configured for a PKI entity.

To uniquely identify an applicant, you can run the following optional commands to configure the alias name for the PKI entity. If you do not configure alias names

 Copyright © Huawei Technologies Co., Ltd. 

for the PKI entities that have the same common name, each of them will fail to apply for a certificate.

**Step 4** (Optional) Run **ip-address** [ **unstructed-address** ] { *ipv4-address* | *interface-type interface-number* }

An IP address is configured for the PKI entity.

By default, no IP address is configured for a PKI entity.

If the **enrollment-request specific** command is executed, the **unstructed-name** parameter can be specified for the PKI entity.

**Step 5** (Optional) Run **fqdn** [ **unstructed-name** ] *fqdn-name*

A fully qualified domain name (FQDN) is configured for the PKI entity.

By default, no FQDN name is configured for a PKI entity.

If the **enrollment-request specific** command is executed, the **unstructed-name** parameter can be specified for the PKI entity.

**Step 6** (Optional) Run **email** *email-address*

An email address is configured for the PKI entity.

By default, no email address is configured for a PKI entity.

**Step 7** (Optional) Run **country** *country-code*

A country code is configured for the PKI entity.

By default, no country code is configured for a PKI entity.

**Step 8** (Optional) Run **locality** *locality-name*

A geographic area is configured for the PKI entity.

By default, no geographic area is configured for a PKI entity.

**Step 9** (Optional) Run **state** *state-name*

A state name or province name is configured for the PKI entity.

By default, no state name or province name is configured for a PKI entity.

**Step 10** (Optional) Run **organization** *organization-name*

An organization name is configured for the PKI entity.

By default, no organization name is configured for a PKI entity.

**Step 11** (Optional) Run **organization-unit** *organization-unit-name*

A department name is configured for the PKI entity.

By default, no department name is configured for a PKI entity.

**Step 12** (Optional) Run **serial-number**

The serial number of a device is added to the PKI entity.

By default, the serial number of a device is not added to the PKI entity.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## 16.7.1.2 Configuring an RSA Key Pair

### Context

Local certificates are signed and issued by the CA. A local certificate is a bundle of public key and PKI entity. Therefore, before applying for a local certificate, you must configure the RSA key pair to generate public and private keys. The public key is sent by the PKI entity to CA, and the peer uses this key to encrypt plaintext. The private key is kept by the PKI entity itself, and the PKI entity uses it to digitally sign and decrypt the ciphertext from peer.

You can configure an RSA key pair using either of the following methods:

- Create an RSA key pair.

  You can directly create a key pair on the device, removing the need to import the key pair to the device memory.
- Import an RSA key pair.

  To use the key pair generated by another PKI entity, upload the key pair to the device through FTP or SFTP and then import it into the device memory. Otherwise, the key pair does not take effect on the device.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run the following commands as required.

- Create an RSA key pair.

  Run **pki rsa local-key-pair create** *key-name* [ **modulus** *modulus-size* ] [ **exportable** ]

  An RSA key pair is created to apply for a local certificate.
- Import an RSA key pair.

  Run **pki import rsa-key-pair** *key-name* { **pem** | **pkcs12** } *file-name* [ **exportable** ] [ **password** *password* ]

  Or run **pki import rsa-key-pair** *key-name* **der** *file-name* [ **exportable** ]

  The specified RSA key pair and certificate in the specified file are imported into the device memory.

  **NOTE**

  Only when the **exportable** parameter is specified in the command, the imported RSA key pair can be exported.

  Windows Server 2003 has a low processing performance. When the device is connected to a Windows Server 2003, the device cannot have too many entities configure or use the key pair with a large size. Otherwise, the device may fail to connect to the server.

**----End**

### Follow-up Procedure

- To back up RSA key pairs or use RSA key pairs on other devices, run the **pki export rsa-key-pair** *key-name* [ **and-certificate** *certificate-name* ] { **pem**

 Copyright © Huawei Technologies Co., Ltd. 

*file-name* [ **3des** | **aes** | **des** ] | **pkcs12** *file-name* } **password** *password* command to export the specified RSA key pair into the device memory. In addition to the RSA key pair, its associated certificate will also be exported. Subsequently, the RSA key pair can be obtained using FTP or SFTP.

- When RSA key pairs are leaked, damaged, lost or not used, run the **pki rsa local-key-pair destroy** *key-name* command to destroy a specified RSA key pair.

  After this command is executed, the specified RSA key pair is deleted from the active device, and it is also deleted from the standby device.
- To check the RSA key pair corresponding to a certificate, run the **pki match-rsa-key certificate-filename** *file-name* command to configure a device to search for the RSA key pair associated with a specific certificate.

## 16.7.1.3 Configuring a PKI Entity to Obtain a CA Certificate

## Context

When applying for a local certificate, the PKI entity sends the certificate enrollment request to the CA. To improve transmission security, the PKI entity must use the CA's public key to encrypt the certificate enrollment message. Therefore, the PKI entity must have the CA's certificate and obtain the public key from the CA certificate.

NOTE

The CA and local certificates have been set in the **default** domain when a device is delivered. To view the CA certificate information, run the **display pki certificate ca realm** *default* command.

## Configuration Procedure

A PKI entity must download and then install a CA certificate.

### 16.7.1.3.1 Downloading a CA Certificate for a PKI Entity

## Context

Several methods are available to download a CA certificate, depending on the service types provided by the CA:

- Download the CA certificate from the CA server through SCEP into the device storage.
- Download the CA certificate from the web server to the device storage through HTTP.
- Download the CA certificate from the server where the certificate is stored to the device storage through LDAP.
- Download the CA certificate from the CMPv2 server through CMPv2 into the device storage.
- Obtain the CA certificate in an outbound way (web, disk, or email) and then upload it to the device storage.

 Copyright © Huawei Technologies Co., Ltd. 

If a PKI entity applies for a local certificate through CMPv2, the root certificate of the CA server is downloaded.

## Procedure

- Download a CA certificate through SCEP.

  For the configuration about downloading CA certificate through SCEP, see **16.7.2.1 Applying for and Updating the Local Certificate Through SCEP**.
- Download a CA certificate through the Hypertext Transfer Protocol (HTTP).
  a. Run **system-view**

     The system view is displayed.
  b. Run **pki http** [ **esc** ] *url-address save-name*

     A CA certificate is downloaded through HTTP.

     *url-address* must include a complete certificate file name and file name extension, for example, http://10.1.1.1:8080/cert.cer. If *url-address* specifies a domain name, ensure that the domain name can be resolved.
- Download a CA certificate through the Lightweight Directory Access Protocol (LDAP).
  a. Run **system-view**

     The system view is displayed.
  b. Run **pki ldap ip** *ip-address* **port** *port* **version** *version* [ **attribute** *attr-value* ] [ **authentication** *ldap-dn ldap-password* ] *save-name* **dn** *dn-value*

     A CA certificate is downloaded through LDAP.
- Download a CA certificate through CMPv2.

  For the configuration about downloading CA certificate through CMPv2, see **16.7.2.2 Applying for and Updating the Local Certificate Through CMPv2**.
- Download a CA certificate in an outbound way.

  After you obtain a CA certificate in an outbound way (web, disk, or email), manually upload it to the device storage. You can also download a CA certificate through the administrator's PC and then upload it to the device storage through FTP or SFTP, or web system.

**----End**

### 16.7.1.3.2 (Optional) Installing a CA Certificate for a PKI Entity

## Context

A downloaded CA certificate must be imported into the device memory to take effect. The device will store the imported certificate file to the **ca_config.ini** file in the default directory and automatically load the certificate file after restarting.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

To prevent a failure to install the CA certificate, ensure that the CA certificate file size does not exceed 1 MB.

When the SCEP is used, the device automatically installs the CA certificate, and you do not need to manually install the CA certificate.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **pki import-certificate** { **ca realm** *realm-name* { **der** | **pkcs12** | **pem** } [ **filename** *filename* ] [ **replace** ] [ **no-check-validate** ] [ **no-check-hash-alg** ] | **realm** *realm-name* **pem terminal password** *password* }

Or run **pki import-certificate ca realm** *realm-name* **pkcs12 filename** *filename* [ **no-check-validate** ] [ **no-check-hash-alg** ] **password** *password*

The CA certificate is imported into the device memory.

**Step 3** (Optional) Run **pki set-certificate expire-prewarning** *day*

The expiry prewarning time of the CA certificate in the device memory is configured.

The default expiry prewarning time of the CA certificate in the device memory is 7 days.

**----End**

## Follow-up Procedure

- To copy a CA certificate to another device, run the **pki export-certificate ca realm** *realm-name* { **der** | **pem** | **pkcs12** } command. Subsequently, the CA certificate is exported into the device storage. Subsequently, the CA certificate can be obtained through FTP or SFTP.
- To copy a default built-in CA certificate to another device, run the **pki export-certificate default ca filename** *filename* command. Subsequently, the default built-in CA certificate is exported into the device storage. Subsequently, the CA certificate can be obtained through FTP or SFTP.
- If a CA certificate expires or is not in use, run the **pki delete-certificate ca realm** *realm-name* command to delete the CA certificate from the device memory.

# 16.7.1.4 Verifying the Local Certificate Preconfiguration

## Prerequisites

A PKI entity, an RSA key pair, and a CA certificate have been configured.

## Procedure

- Run the **display pki entity** [ *entity-name* ] command to check PKI entity information.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **display pki rsa local-key-pair** { **pem** | **pkcs12** } *filename* [ **password** *password* ] command to check RSA key pair information.
- Run the **display pki rsa local-key-pair** [ **name** *key-name* ] **public** [ **temporary** ] command to check RSA public key information.
- Run the **display pki realm** [ *realm-name* ] command to check PKI realm information.
- Run the **display pki certificate ca realm** *realm-name* command to check the loaded CA certificate.
- Run the **display pki credential-storage-path** command to check the default path where a PKI certificate is stored.
- Run the **display pki ca-capability realm** *realm-name* command to check the CA capabilities of a PKI domain.

**----End**

## 16.7.2 Applying for and Updating Local Certificate

### Context

NOTE

The CA and local certificates have been set in the **default** domain when a device is delivered. To view the local certificate information, run the **display pki certificate local realm** *default* command.

### Prerequisites

The **16.7.1 Preconfiguring a Local Certificate** is complete.

### Configuration Procedure

Select one of the following methods to apply for and update a local certificate.

### 16.7.2.1 Applying for and Updating the Local Certificate Through SCEP

### Context

Two methods are available to apply for the local certificate for a PKI entity through the Simple Certificate Enrollment Protocol (SCEP):

- Automatic local certificate application and update

  If the configuration required for local certificate application has been performed and the device has no local certificate, the device automatically applies for the local certificate through SCEP. Alternatively, if the local certificate will expire soon, has expired, or reaches the specified percentage of validity period, the device automatically applies for and updates the local certificate through SCEP.
- Manual local certificate application

  If the configuration required for local certificate application has been performed and the device has no local certificate, the device is manually triggered to apply for the local certificate through SCEP. If the local certificate

 Copyright © Huawei Technologies Co., Ltd. 

will expire soon, has expired, or reaches the specified percentage of validity period, the device does not automatically apply for and update the local certificate through SCEP.

When you use either of the two methods to apply for the local certificate, the device obtains the CA certificate, saves it to the device storage and automatically imports it to the device memory. Then the device uses the public key in the CA certificate to encrypt its local certificate enrollment request and sends it to CA to apply for a local certificate. Finally the device saves the local certificate to the device storage and imports it to the device memory automatically.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **pki file-format** { **der** | **pem** }

The file format in which the device stores the certificate is configured.

By default, the device stores the certificate into a PEM file.

**Step 3** Run **pki realm** *realm-name*

A PKI realm is created and the PKI realm view is displayed; or the PKI realm view is displayed directly.

By default, the device has a PKI realm named **default**. This realm can only be modified but cannot be deleted.

A PKI realm is valid only on the local device and unavailable to certificate authorities (CAs) or other devices. Each PKI realm has its own parameters.

**Step 4** Run **ca id** *ca-name*

A trusted CA is configured for the PKI realm.

By default, no trusted CA is configured for a PKI realm.

*ca-name* specifies the name of a CA server.

**Step 5** Run **entity** *entity-name*

A PKI entity that applies for a local certificate is specified.

By default, no PKI entity that applies for a local certificate is specified.

The PKI entity specified by *entity-name* must have been created using the **pki entity** command.

**Step 6** Run **rsa local-key-pair** *key-name*

The RSA key pair used in SCEP-based certificate application is configured.

By default, the RSA key pair used in SCEP-based certificate application is not configured.

The RSA key pair specified by *key-name* must have been created using the **pki rsa local-key-pair create** command.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 7** (Optional) Run **key-usage** { **ike** | **ssl-client** | **ssl-server** } *

The certificate public key usage attribute is configured.

By default, no certificate public key usage attribute is configured.

**Step 8** (Optional) Run **source interface** *interface-type interface-number*

The source interface used in TCP connection setup is specified.

By default, the source interface used in a TCP connection is an egress interface.

The source interface must be a Layer 3 interface with an IP address configured.

**Step 9** (Optional) Run **enrollment-request specific**

The device is configured to use a certificate request packet of a specific format to apply for a certificate from the CA server.

By default, the device uses a certificate request packet of the standard format to apply for a certificate from the CA server.

**Step 10** (Optional) Run **extension-request enterprise**

The extended attribute in the certificate enrollment request carries the object ID defined by Verisign.

By default, the extended attribute in the certificate enrollment request carries the object ID defined by PKCS#9.

To insert the object ID defined by Verisign into the local certificate extended attribute, run this command.

**Step 11** Run **enrollment-url** [ **esc** ] *url* [ **interval** *minutes* ] [ **times** *count* ] [ **ra** ]

A CA server URL is configured.

By default, the CA server URL is not configured.

Pay attention to the following points:

- If the **esc** parameter is not specified in the command, the URL format is **http://*server_location*/*ca_script_location***.

  *server_location* supports the IP address format or domain name format. *ca_script_location* is the path where CA server host's application script is located. For example, when the Windows server functions as the CA server, the URL format is **http://*host*:*port*/certsrv/mscep/mscep.dll**. *host* is the CA server's IP address, and *port* is the CA server's port number. If the CA server's IP address is 10.1.1.1 and port number is 8080, the URL is **http://10.1.1.1:8080/certsrv/mscep/mscep.dll**.
- If the **esc** parameter is specified, the URL that contains a question mark (?) can be entered in ASCII format.

  The **esc** parameter is specified to allow a URL that contains a question mark (?) to be entered in ASCII format. The URL must be in \x3f format, in which 3f is a hexadecimal ASCII value of question mark (?). For example, if a user wants to enter http://***.com?page1, the corresponding URL is http://***.com\x3fpage1. If the user also wants to enter question mark (?) and \x3f (http://www.***.com?page1\x3f), the corresponding URL is **http://www.***.com\x3fpage1\\x3f**.

 Copyright © Huawei Technologies Co., Ltd. 

- If certificate requests are manually processed on the CA server, it may take a long period of time to issue a certificate. The PKI entity applying for a certificate needs to periodically send queries to obtain the issued certificate in time. To adjust the certificate enrollment query interval and maximum number of queries, configure the **interval** and **times** parameters.
- If the **ra** parameter is specified, an RA authenticates a PKI entity's identity information during local certificate application. By default, a CA authenticates a PKI entity's identity information during local certificate application.

**Step 12** Run **enrollment-request signature message-digest-method** { **md5** | **sha1** | **sha-256** | **sha-384** | **sha-512** }

The digest algorithm used to sign certificate enrollment requests is configured.

By default, the digest algorithm used to sign certificate enrollment requests is **sha-256**.

SHA2 algorithms are more secure than **md5** and **sha1** algorithms and so are recommended.

The digest algorithm used on a PKI entity must be the same as that used on the CA server.

**Step 13** Run **password cipher** *password*

The challenge password used in SCEP certificate application is configured. The challenge password is also called certificate revocation password.

By default, the challenge password used in SCEP certificate application is not configured.

The challenge password used on a PKI entity must be the same as that configured on the CA server. If the CA server does not require a challenge password, this challenge password does not need to be configured.

**Step 14** Run **fingerprint** { **md5** | **sha1** | **sha256** } *fingerprint*

The CA certificate fingerprint used in CA certificate authentication is configured.

By default, the CA certificate fingerprint used in CA certificate authentication is not configured.

The fingerprint needs to be obtained offline from a CA server. For example, when Windows Server 2008 functions as the CA server, access the web page address http://*host:port*/certsrv/mscep_admin/ to obtain the CA certificate fingerprint. In the web page address, *host* specifies the CA server's IP address, and *port* specifies the CA server's port number.

**Step 15** Configure the local certificate application and update mode.

- Configure automatic application and update of local certificate.

  Run **auto-enroll** [ *percent* ] [ **regenerate** [ *key-bit* ] ] [ **updated-effective** ]

  The automatic certificate application and update function is enabled.

  By default, the automatic certificate application and update function is disabled.
- Configure manual local certificate application.

  a. Run **quit**

 Copyright © Huawei Technologies Co., Ltd. 

Return to the system view.

b. Run **pki enroll-certificate realm** *realm-name* [ **password** *password* ]

Manual certificate application is configured.

If the **password** command is configured, the **password** parameter does not need to be specified. If both the **password** command and **password** parameter are configured, the **password** parameter setting takes effect.

**----End**

## 16.7.2.2 Applying for and Updating the Local Certificate Through CMPv2

## Context

If the device can access a CA and the CA supports the Certificate Management Protocol version 2 (CMPv2), the device can apply for and update the local certificate through CMPv2.

CMPv2-based local certificate application applies to the following situations:

- Initial local certificate application using an initialization request (IR)

  The device sends the CA an IR to apply for the local certificate for the first time. In this situation, the device shows its identity to the CMPv2 server in either of the following ways:

  – Message authentication code: The device and CMPv2 server share a pair of message authentication code's reference values and secret values. When applying for the local certificate for the first time, the device adds this pair of reference values and key values to a certificate request and sends the request to the CMPv2 server. The CMPv2 server validates the reference values and secret values to authenticate the device.

  – Signature: The device sends an IR to the CA to initiate a certificate request and uses the private key for the certificate issued by another CA for signature protection.

- Local certificate application for another device using a certification request (CR)

  The device has the local certificate issued by the CA and needs to apply for an additional local certificate for another device. In this situation, the device uses the existing certificate for identity authentication.

CMPv2 supports two local certificate update modes:

- Manual certificate update using a key update request (KUR)

  A KUR, also called certificate update request, is used to update the device's existing certificate that has not expired and not revoked. During local certificate update, the device uses the existing certificate for identity authentication. The device can use the new or previous public key to update the local certificate.

  Applying for a local certificate using an IR is insecure. You are advised to update the local certificate and key pair using a KUR.

- Automatic certificate update

  The device must apply for a new certificate before the existing certificate expires to prevent service interruptions. In manual certificate update mode,

 Copyright © Huawei Technologies Co., Ltd. 

the device is more likely to forget certificate update. To avoid this problem, the device supports automatic certificate update. When the system detects that the certificate automatic update time expires, the system initiates a certificate update request to the CMPv2 server. The obtained new certificate will replace the certificate file in the device storage and certificate in the device memory without interrupting services.

This method can be used to automatically update the local certificate obtained using an IR or updated using a KUR.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **pki file-format** { **der** | **pem** }

The file format in which the device stores the certificate is configured.

By default, the device stores the certificate into a PEM file.

**Step 3** Run **pki realm** *realm-name*

A PKI realm is created and the PKI realm view is displayed; or the PKI realm view is displayed directly.

By default, no PKI realm is created.

**Step 4** Run **quit**

Return to the system view.

**Step 5** Run **pki cmp session** *session-name*

A CMP session is created and the CMP session view is displayed; or the CMP session view is displayed directly.

By default, no CMP session is created.

A CMP session is valid only on the local device and is unavailable to the CA and other devices.

**Step 6** Run **cmp-request entity** *entity-name*

The PKI entity name used in CMPv2-based certificate application is configured for the device.

By default, the pki entity name used in CMPv2-based certificate application is not configured.

**Step 7** Run **cmp-request ca-name** *ca-name*

The CA name is configured for the CMP session.

By default, no CA name is configured for a CMP session.

The sequence of each field in the configured CA name must be the same as that in the CA certificate. Otherwise, the CMPv2 server considers the CA name incorrect.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 8** Run **cmp-request server url** [ **esc** ] *url-addr*

The CMPv2 server URL is configured.

By default, the CMPv2 server URL is not configured.

*url-addr* can be the IP address or domain name format. If it is set to the domain name format, Domain Name System (DNS) must be correctly configured on a PKI entity so that the pki entity can resolve the domain name through the DNS server.

**Step 9** Run **cmp-request rsa local-key-pair** *key-name* [ **regenerate** [ *key-bit* ] ]

The RSA key pair used in CMPv2-based certificate application is configured.

By default, the RSA key pair used in CMPv2-based certificate application is not configured.

If the **regenerate** parameter is specified, the system generates a new RSA key pair to apply for a new certificate and uses the new certificate and RSA key pair to replace the previous ones during automatic certificate update. Otherwise, the system continues to use the previous RSA key pair during automatic certificate update.

**Step 10** Run **cmp-request realm** *realm-name*

The PKI realm used in CMPv2-based certificate application is configured.

By default, the PKI realm used in CMPv2-based certificate application is not configured.

**Step 11** (Optional) Run **cmp-request verification-cert** *cert-file-name*

The certificate file used to validate the CA response signature is configured.

By default, the certificate file used to validate the CA response signature is not configured.

- If this command is configured and the CMPv2 server signs its certificate response, the device uses the certificate configured using this command to validate the server's response signature. The configured certificate is a CA certificate used to verify a CA's identity.
- If this command is not configured and the CMPv2 server signs its certificate response, the device uses the certificates on the device and in the server's response to build a certificate chain and then validate the server's response signature. If the server uses the message authentication code to authenticate packets, the device uses the configured message authentication code to validate the server's response packet.

**Step 12** Apply for the local certificate according to the actual situation.

- Initial local certificate application using an IR
  a. Run **cmp-request origin-authentication-method** { **message-authentication-code** | **signature** }

     The authentication mode of CMPv2-based initial local certificate application is configured.

     By default, the authentication mode of CMPv2-based initial local certificate application is message authentication code.

 Copyright © Huawei Technologies Co., Ltd. 

- **message-authentication-code** specifies the message authentication code mode. When this mode is selected, perform **Step 12.b**.
- **signature** specifies the signature mode. When this mode is selected, perform **Step 12.c**.

b. Run **cmp-request message-authentication-code** *reference-value secret-value*

The message authentication code's reference values and secret values are configured.

By default, the message authentication code's reference values and secret values are not configured.

The message authentication code's reference values and secret values need to be obtained from the CMPv2 server in an outband way.

c. Run **cmp-request authentication-cert** *cert-name*

The certificate carried in a CMPv2 request for identity authentication is configured.

By default, the certificate carried in a CMPv2 request for identity authentication is not configured.

This certificate is an additional certificate and must be issued by another trusted certificate authority.

d. Run **quit**

Return to the system view.

e. Run **pki cmp initial-request session** *session-name*

The device sends an IR to apply for the local certificate with the CMPv2 server according to the CMP session configuration for the first time.

After this command is configured, the system first checks the CMP session configuration to determine whether it can apply for the local certificate. If the condition is not met, an error message is displayed. If the condition is met, the system initiates an initial certificate request according to the configuration. The obtained certificate is saved in a file to the device storage without being imported into the memory. If the server provides a CA certificate in a response, the CA certificate is also saved in a file.

- Local certificate application for another device using a CR

a. Run **cmp-request authentication-cert** *cert-name*

The certificate carried in a CMPv2 request for identity authentication is configured.

By default, the certificate carried in a CMPv2 request for identity authentication is not configured.

This certificate is the local certificate that the CA has issued to the device.

b. Run **quit**

Return to the system view.

c. Run **pki cmp certificate-request session** *session-name*

The device sends a CR to apply for the local certificate with the CMPv2 server according to the CMP session configuration.

 Copyright © Huawei Technologies Co., Ltd. 

After this command is configured, the system first checks the CMP session configuration to determine whether it can update the local certificate. If the condition is not met, an error message is displayed. If the condition is met, the system initiates a certificate update request according to the configuration. The obtained certificate is saved in a file to the device storage without being imported into the memory.

**Step 13** Update the local certificate according to the actual situation.

- Manual certificate update using a KUR
  a. Run **pki cmp session** *session-name*

     The CMP session view is displayed directly.
  b. Run **cmp-request authentication-cert** *cert-name*

     The certificate carried in a CMPv2 request for identity authentication is configured.

     By default, the certificate carried in a CMPv2 request for identity authentication is not configured.

     This certificate is the local certificate that the CA has issued to the device and needs to be replaced by a new local certificate.
  c. Run **quit**

     Return to the system view.
  d. Run **pki cmp keyupdate-request session** *session-name*

     The device sends the CMPv2 server a KUR to update the key according to the CMP session configuration.

     When the device requests to update the key with the CMPv2 server, it also applies for a new local certificate.

     After this command is configured, the system first checks the CMP session configuration to determine whether it can update the local certificate. If the condition is not met, an error message is displayed. If the condition is met, the system initiates a certificate update request according to the configuration. The obtained certificate is saved in a file to the device storage without being imported into the memory.
- Automatic certificate update
  a. Run **pki cmp session** *session-name*

     The CMP session view is displayed directly.
  b. Run **cmp-request authentication-cert** *cert-name*

     The certificate carried in a CMPv2 request for identity authentication is configured.

     By default, the certificate carried in a CMPv2 request for identity authentication is not configured.

     This certificate is the local certificate that the CA has issued to the device and needs to be replaced by a new local certificate.
  c. Run **certificate auto-update enable**

     The CMPv2-based automatic certificate update function is enabled.

     By default, the CMPv2-based automatic certificate update function is disabled.

 Copyright © Huawei Technologies Co., Ltd. 

d. Run **certificate update expire-time** *valid-percent*

The time when the local certificate is updated automatically is configured. The value is expressed as the percentage of the certificate validity period.

The default certificate update time is 50% of the certificate validity period.

After this command is configured, the system initiates a certificate update request and determines whether to create a new RSA key pair according to the **cmp-request rsa local-key-pair** command configuration when finding that the automatic certificate update time reaches the value specified by *valid-percent*. After the new certificate is obtained, the system replaces the previous certificate and RSA key pair with the new ones.

e. Run **quit**

Return to the system view.

**Step 14** (Optional) Run **undo pki cmp poll-request session** *session-name*

The ongoing CMP poll request is cancelled.

If the server cannot respond to the client within a specified period after the client initiates a certificate-related request, the server requires the client to send a poll request at an interval until it responds to the client. If the client does not want to wait, it can cancel the ongoing CMP poll request to cancel certificate application.

**----End**

## 16.7.2.3 Applying for the Local Certificate in Offline Mode

## Context

If the CA server does not support SCEP or CMPv2, configure the device to apply for the local certificate in offline mode. Users generate a certificate request file on the device and then send the file to the CA in an outbound way (web, disk, or email) to apply for the local certificate. After applying for the certificate, users still need to download the certificate from the server where the certificate is stored and save it to the device storage.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **pki realm** *realm-name*

A PKI realm is created and the PKI realm view is displayed; or the PKI realm view is displayed directly.

By default, the device has a PKI realm named **default**. This realm can only be modified but cannot be deleted.

A PKI realm is valid only on the local device and unavailable to certificate authorities (CAs) or other devices. Each PKI realm has its own parameters.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 3** Run **entity** *entity-name*

A PKI entity that applies for a local certificate is specified.

By default, no PKI entity that applies for a local certificate is specified.

The PKI entity specified by *entity-name* must have been created using the **pki entity** command.

**Step 4** Run **rsa local-key-pair** *key-name*

The RSA key pair used in offline mode certificate application is configured.

By default, the RSA key pair used in offline mode certificate application is not configured.

**Step 5** Run **enrollment-request signature message-digest-method** { **md5** | **sha1** | **sha-256** | **sha-384** | **sha-512** }

The digest algorithm used to sign certificate enrollment requests is configured.

By default, the digest algorithm used to sign certificate enrollment requests is **sha-256**.

Other algorithms are more secure than **md5** and **sha1** algorithms and so are recommended.

The digest algorithm used on a PKI entity must be the same as that used on the CA server.

**Step 6** (Optional) Run **key-usage** { **ike** | **ssl-client** | **ssl-server** } *

The certificate public key usage attribute is configured.

By default, no certificate public key usage attribute is configured.

**Step 7** (Optional) Run **enrollment-request specific**

The device is configured to use a certificate request packet of a specific format to apply for a certificate from the CA server.

By default, the device uses a certificate request packet of the standard format to apply for a certificate from the CA server.

**Step 8** (Optional) Run **extension-request enterprise**

The extended attribute in the certificate enrollment request carries the object ID defined by Verisign.

By default, the extended attribute in the certificate enrollment request carries the object ID defined by PKCS#9.

To insert the object ID defined by Verisign into the local certificate extended attribute, run this command.

**Step 9** Run **quit**

Return to the system view.

**Step 10** Run **pki file-format** { **der** | **pem** }

The file format in which the device stores the certificate and certificate request is configured.

 Copyright © Huawei Technologies Co., Ltd. 

By default, the device stores the certificate and certificate request into a PEM file.

**Step 11** Run **pki enroll-certificate realm** *realm-name* **pkcs10** [ **filename** *filename* ] [ **password** *password* ]

The device is configured to save certificate application information into a file in PKCS#10 format.

The challenge password used on a PKI entity must be the same as that configured on the CA server. If the CA server does not require a challenge password, this challenge password does not need to be configured.

**Step 12** Enable the device to send the CA the certificate request file in an outbound way (web, disk, or email) to apply for the local certificate.

**----End**

### 16.7.2.4 Verifying the Local Certificate Application and Update Configuration

#### Prerequisites

The local certificate application and update configuration has been completed.

#### Procedure

- Run the **display pki realm** [ *realm-name* ] command to check PKI realm information.
- Run the **display pki credential-storage-path** command to check the default path where a PKI certificate is stored.
- Run the **display pki certificate enroll-status** [ **realm** *realm-name* ] command to check the certificate enrollment status.
- Run the **display pki cert-req filename** *file-name* command to check the certificate request file.
- Run the **display pki cmp statistics** [ **session** *session-name* ] command to check CMP session statistics.
- Run the **display pki certificate** { **ca** | **local** } **realm** *realm-name* command to check the loaded CA certificate and local certificate.

**----End**

## 16.7.3 (Optional) Downloading a Local Certificate

#### Context

If the device applies for the local certificate through SCEP or CMPv2, it automatically downloads the local certificate. The local certificate needs to be downloaded only when the local certificate is applied for in offline mode.

The device often obtains the local certificate using the following methods depending on the service types provided by the CA server:

- Download the local certificate from the web server to the device storage through HTTP.

 Copyright © Huawei Technologies Co., Ltd. 

- Download the local certificate from the server where the certificate is stored to the device storage through LDAP.
- Obtain the local certificate in an outbound way (web, disk, or email) and then upload it to the device storage.

### Prerequisites

The device has applied for the local certificate in offline mode, and the local certificate has been enrolled on the CA successfully.

### Procedure

- Download the local certificate through HTTP.
  a. Run **system-view**

     The system view is displayed.
  b. Run **pki http** [ **esc** ] *url-address save-name*

     The device is configured to download the local certificate through HTTP.

     *url-address* must include a complete certificate file name and file name extension, for example, http://10.1.1.1:8080/cert.cer. If *url-address* specifies a domain name, ensure that the domain name can be resolved.
- Download the local certificate through LDAP.
  a. Run **system-view**

     The system view is displayed.
  b. Run **pki ldap ip** *ip-address* **port** *port* **version** *version* [ **attribute** *attr-value* ] [ **authentication** *ldap-dn ldap-password* ] *save-name* **dn** *dn-value*

     The device is configured to download the local certificate through LDAP.
- Download the local certificate in an outbound way (web, disk, or email).

  After you obtain the local certificate in an outbound way (web, disk, or email), manually upload it to the device storage. You can also download the local certificate through the administrator's PC and then upload it to the device storage through FTP or SFTP, or web system.

**----End**

### Verifying the Configuration

- Run the **display pki credential-storage-path** command to check the default path where a PKI certificate is stored.
- Run the **dir (user view)** command to check the local certificate file in a storage device.

## 16.7.4 (Optional) Installing the Local Certificate

### Context

The downloaded local certificate must be imported into the device memory to take effect. The device will store the imported certificate file to the **ca_config.ini**

 Copyright © Huawei Technologies Co., Ltd. 

file in the default directory and automatically load the certificate file after restarting.

## Prerequisites

The local certificate has been downloaded, and the certificate file has been stored to the device storage.

NOTE

To prevent a failure to install the local certificate, ensure that the certificate file size does not exceed 1 MB.

You need to manually install the local certificate when the local certificate is applied offline or the CMPv2 method is configured. When the SCEP method is configured, the device automatically downloads the local certificate.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **pki import-certificate** { **local realm** *realm-name* { **der** | **pkcs12** | **pem** } [ **filename** *filename* ] [ **replace** ] [ **no-check-validate** ] [ **no-check-hash-alg** ] | **realm** *realm-name* **pem terminal password** *password* }

Or run **pki import-certificate local realm** *realm-name* **pkcs12 filename** *filename* [ **no-check-validate** ] [ **no-check-hash-alg** ] **password** *password*

The local certificate is imported into the device memory.

A key pair file may be included in the certificate file, or exist independently of the certificate file. The import methods are different.

- A certificate file contains a key pair file.

  Run the **pki import rsa-key-pair** command to import the certificate and key pair files simultaneously.

  NOTE

  If a certificate file contains a key pair file, the **pki import-certificate** command imports only the certificate file, but not the key pair file. To import the key pair file, run the **pki import rsa-key-pair** command after the **pki import-certificate** command.

- The key pair file is independent of the certificate file.

  a. Import the certificate file.

     Run the **pki import-certificate** command.

  b. Import the key pair file.

     Run the **pki import rsa-key-pair** command.

**Step 3** (Optional) Run **pki set-certificate expire-prewarning** *day*

The expiry prewarning time of the local certificate in the device memory is configured.

 Copyright © Huawei Technologies Co., Ltd. 

The default expiry prewarning time of the local certificate in the device memory is 7 days.

**----End**

### Follow-up Procedure

- To copy the local certificate to another device, run the **pki export-certificate local realm** *realm-name* { **der** | **pem** | **pkcs12** } command. Subsequently, the local certificate is exported into the device storage. Subsequently, the local certificate can be obtained through FTP or SFTP.
- To copy a default built-in local certificate to another device, run the **pki export-certificate default local filename** *filename* command. Subsequently, the default built-in local certificate is exported into the device storage. Subsequently, the local certificate can be obtained through FTP or SFTP.

### Verifying the Configuration

Run the **display pki certificate local realm** *realm-name* command to check the loaded local certificate.

## 16.7.5 Verifying the CA and Local Certificates

### Prerequisites

The task of **16.7.4 (Optional) Installing the Local Certificate** is complete.

### Configuration Procedure

Perform the following operations in sequence:

### 16.7.5.1 Configuring Local Certificate Check

### Context

The PKI entity periodically validates the peer certificate, for example, whether the peer certificate expires and whether it is added to CRL. There are three ways to check certificate status: CRL, OCSP, and None.

- CRL

  If the CA server can function as a CRL distribution point (CDP), the certificate issued by CA contains the CDP information about obtaining the certificate CRL. The PKI entity then uses the specified method (HTTP or LDAP) to find out the CRL from the specified location and download the CRL.

  If the CDP URL is configured for a PKI entity, the PKI entity obtains the CRL from the specified URL. If the CA server cannot function as a CDP, the PKI entity uses SCEP to download the CRL.

  When the PKI entity authenticates the local certificate, the PKI entity searches for the certificate in the CRL stored in local memory. If the certificate is included in the CRL, it indicates that the certificate has been revoked. If no CRL is available in local memory, the CRL needs to be downloaded and installed.

 Copyright © Huawei Technologies Co., Ltd. 

- OCSP

  When two PKI entities use certificates to perform IPSec negotiation, they check the peer certificate status through OCSP in real time.

  OCSP does not require the PKI entity frequently download CRL. When a PKI entity accesses an OCSP server, the entity requests the certificate status. The OCSP server replies with a valid, expired, or unknown state.

  - Valid indicates that the certificate has not been revoked.
  - Expired indicates that the certificate has been revoked.
  - Unknown indicates that the OCSP server does not know the certificate status.

- None

  If no CRL or OCSP server is available to the PKI entity or the PKI entity does not need to check the local certificate status, this mode can be used. In this mode, the PKI entity does not check certificate revocation.

## Procedure

1. Run **system-view**

   The system view is displayed.

2. Run **pki realm** *realm-name*

   A PKI realm is created and its view is displayed, or the view of an existing PKI realm is displayed.

   By default, the device has a PKI realm named **default**. This realm can only be modified but cannot be deleted.

3. Run **certificate-check** { { **crl** | **ocsp** } * [ **none** ] | **none** }

   The method to check whether certificate revocation is configured in the PKI realm.

   By default, the system checks using CRLs whether a certificate in the PKI realm is revoked.

   If multiple certificate status check methods are configured, these methods are used in the configuration sequence. The later method is used only when the previous method is unavailable because, for example, the server cannot be connected. If None is configured, a certificate is considered valid when all the previous methods are unavailable. For example, after the **certificate-check crl ocsp none** command is executed, the PKI entity uses CRL to check certificate status first. If the CRL method is unavailable, the PKI entity uses OCSP. If neither CRL nor OCSP is available, the certificate is considered valid.

4. Select a method to check peer certificate status according to the service types provided by the CA:
   - **Automatic CRL Update**
   - **Manual CRL Update**
   - **OCSP**

## Automatic CRL Update

1. Run **quit**

   Return to the system view.

 Copyright © Huawei Technologies Co., Ltd. 

2. (Optional) Run **pki file-format** { **der** | **pem** }
   The format of saved CRL is set.
   By default, CRL is saved in PEM format.
3. Run **pki realm** *realm-name*
   The view of an existing PKI realm is displayed.
4. Run **crl auto-update enable**
   Automatic CRL update is enabled.
   By default, automatic CRL update is enabled.
5. Run **crl update-period** *interval*
   The interval for automatic CRL update is set.
   By default, the automatic CRL update interval is 8 hours.
6. Select an automatic CRL update method according to the service types provided by the CA.
   - SCEP
     i. Run **crl scep**
        The CRL is automatically updated using SCEP.
        By default, CRL is automatically updated using HTTP.
     ii. Run **cdp-url** [ **esc** ] *url-addr*
        The CDP URL is configured
        By default, no CDP URL is configured.
   - HTTP
     i. Run **crl http**
        The CRL is automatically updated using HTTP.
        By default, CRL is automatically updated using HTTP.
     ii. Run **cdp-url** [ **esc** ] *url-addr*
        The CDP URL is configured.
        Or run **cdp-url from-ca**
        The device is configured to obtain CDP URL from the CA certificate.
        By default, no CDP URL is configured.
   - LDAP
     i. Run **crl ldap**
        The CRL is automatically updated using LDAP.
        By default, CRL is automatically updated using HTTP.
     ii. Run **ldap-server** { **authentication** *ldap-dn ldap-password* | **ip** *ip-address* [ **port** *port* | **version** *version* ] * }
        The CRL is automatically updated using LDAP.
        By default, no LDAP server is configured.
     iii. Run **crl ldap** [ **attribute** *attr-value* ] **dn** *dn-value*
        The attributes and identifier used to obtain CRL from the LDAP server are configured.
        By default, no attributes and identifier used to obtain CRL from the LDAP server are configured.

 Copyright © Huawei Technologies Co., Ltd. 

- LDAPv3
  i. Run **quit**

     Return to the system view.
  ii. Run **ldap-server template** *template-name*

     By default, no LDAP server template exists on the device.
  iii. Run **ldap-server authentication** *ip-address* [ *port-number* ]

     An LDAP authentication server is created.

     By default, no LDAP authentication server is configured.
  iv. Run **ldap-server authentication manager** *manager-dn password* [ *repassword* ]

     The administrator DN and password of an LDAP authentication server are configured.

     By default, no administrator DN and password of an LDAP authentication server is configured.

     After the configuration is complete, run the **ldap-server authentication manager-password** *password* [ *repassword* ] to change the administrator password of the LDAP authentication server.
  v. Run **quit**

     Return to the system view.
  vi. Run **pki realm** *realm-name*

     The view of an existing PKI realm is displayed.
  vii. Run **crl ldap**

     The CRL is automatically updated using LDAP.

     By default, CRL is automatically updated using HTTP.
  viii. Run **ldap-server-template** *attr-value*

     An LDAP server template is bound to a PKI realm.

     By default, no LDAP server template is bound to a PKI realm.

     The *attr-value* value is specified in the **ldap-server template** command.

7. Run **crl cache**

   The PKI realm is allowed to use the CRL in cache.

   By default, the PKI realm is allowed to use cached CRLs.
8. (Optional) Update the CRL immediately.
   a. Run **quit**

      Return to the system view.
   b. Run **pki get-crl realm** *realm-name*

      The CRL is immediately updated.

      After this command is executed, the new CRL replaces the old CRL in the storage, and is automatically imported to the memory to replace the old one.

 Copyright © Huawei Technologies Co., Ltd. 

## Manual CRL Update

1. Run **quit**

   Return to the system view.

2. (Optional) Run **pki file-format** { **der** | **pem** }

   The format of saved CRL is set.

   By default, CRL is saved in PEM format.

3. Select a manual CRL update method according to the service types provided by the CA.
   - To download the CRL using HTTP, run the **pki http** [ **esc** ] *url-address save-name* command.

     The value of *url-address* must contain the certificate file name plus the file name extension, for example, http://10.1.1.1:8080/cert.cer cert.cer. If *url-address* specifies a domain name, ensure that the domain name can be resolved.
   - To download the CRL using LDAP, run the **pki ldap ip** *ip-address* **port** *port* **version** *version* [ **attribute** *attr-value* ] [ **authentication** *ldap-dn ldap-password* ] *save-name* **dn** *dn-value* command.

4. Run **pki import-crl realm** *realm-name* **filename** *file-name*

   The CRL is imported to the memory.

## OCSP

1. (Optional) Run **source interface** *interface-type interface-number*

   The source interface used in TCP connection setup is specified.

   By default, the source interface used in TCP connection setup is the egress interface.

   The source interface must be a Layer 3 interface with an IP address configured.

2. Run **ocsp url** [ **esc** ] *url-address*

   The OCSP server's URL is configured.

   Or run **ocsp-url from-ca**

   The device is configured to obtain OCSP server's URL from the CA certificate's AIA option.

   By default, an OCSP server does not have a URL address.

3. (Optional) Run **ocsp nonce enable**

   The nonce extension is added to the OCSP requests sent by the PKI entity.

   By default, the OCSP requests sent by the PKI entity contain the nonce extension.

   The nonce extension improves security and reliability for communication between the PKI entity and OCSP server. The content of a nonce extension is randomly generated by the system. The response packets sent by the OCSP server may contain or not contain the nonce extension. If the response packets contain a nonce extension, it must be the same as that configured for OCSP requests.

4. (Optional) Run **ocsp signature enable**

 Copyright © Huawei Technologies Co., Ltd. 

Signature for OCSP requests is enabled.

By default, signature for OCSP requests is disabled.

This command is required when the OCSP server requests signature for OCSP requests.

5. Run **quit**

   Return to the system view.

6. Run **pki import-certificate ocsp realm** *realm-name* { **der** | **pkcs12** | **pem** } [ **filename** *filename* ]

   Or run **pki import-certificate ocsp realm** *realm-name* **pkcs12 filename** *filename* **password** *password*

   The OCSP server certificate is imported to memory.

7. Run **pki validate ocsp-server-certificate enable**

   The function that uses the OCSP server certificate to verify OCSP server packets is enabled.

   By default, the function that uses the OCSP server certificate to verify OCSP server packets is disabled.

8. Run **pki ocsp response cache enable**

   The OCSP response cache function is enabled.

   By default, the OCSP response cache function is disabled.

   After this command is executed, the PKI entity searches the cache first in checking the certificate status using OCSP. If the cache searching fails, the PKI entity sends a request to the OCSP server. In addition, the PKI entity caches valid OCSP responses for next search.

   An OCSP response has a validity period. After the OCSP response cache function is enabled, the PKI entity updates cached OCSP responses every one minute and deletes the expired responses.

9. (Optional) Run **pki ocsp response cache number** *number*

   The maximum number of OCSP responses in the cache is set.

   By default, a PKI entity can cache 2 OCSP responses.

10. (Optional) Run **pki ocsp response cache refresh interval** *interval*

    The interval at which the PKI entity updates the OCSP response cache is set.

    By default, the PKI entity updates the OCSP response cache every five minutes.

## Follow-up Procedure

- If you want to copy an OCSP server certificate from the local device to another device, run the **pki export-certificate ocsp realm** *realm-name* { **der** | **pem** | **pkcs12** } command to export the certificate file to the local device memory first, and then transfer the certificate file to another device using a file transferring protocol.
- To delete an expired or unused OCSP server certificate from memory, run the **pki delete-certificate ocsp realm** *realm-name* command.
- To delete an expired or unused CRL from memory, run the **pki delete-crl realm** *realm-name* command.

 Copyright © Huawei Technologies Co., Ltd. 

## 16.7.5.2 Checking the CA and Local Certificates

## Context

Before a certificate is used, it must be authenticated. In a certificate, the issuing date, issuer information, and certificate validity need to be authenticated. The key to authenticate a certificate is to check the signature of CA and check whether the certificate is expired or revoked.

In certificate authentication, the local device must obtain the peer certificate and the following information: CA certificate, CRL, local certificate and its private key, and certificate authentication information.

The local device authenticates a local certificate as follows:

1. Uses the public key of the CA certificate to authenticate its signature.

   To authenticate a certificate, a PKI entity must obtain the public key of the CA that issued the certificate from the CA's certificate, so that the PKI entity can check the signature of the CA on the certificate. An upper-level CA authenticates the certificates of lower-level CAs. The authentication is performed along the certificate chain, and terminated at the trustpoint (the root CA holding a self-signed certificate or a subordinate CA trusted by the PKI entity).

   PKI entities sharing the same root or subordinate CA and having CA certificates can authenticate certificates of each other (peer certificates). Authentication of a peer certificate chain ends at the first trusted certificate or CA.

   In a word, certificate chain authentication starts at an entities certificate and ends at a trustpoint.
2. Checks whether the certificate has expired.
3. Checks whether the certificate has been revoked in CRL or None mode.

To check validity of the CA and local certificates of the local device, perform the following steps.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **pki validate-certificate** { **ca** | **local** } **realm** *realm-name*

The validity of CA or local certificate is checked.

The **pki validate-certificate ca** command allows you to verify only the root CA certificate, but not subordinate CA certificates. When multiple CA certificates are imported on a device, you can use only the **pki validate-certificate local** command to verify the validity of subordinate certificates.

**Step 3** (Optional) Run **pki realm** *realm-name*

A PKI realm is created and its view is displayed, or the view of an existing PKI realm is displayed.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 4** (Optional) Run **validate time disable**

The time check in PKI certificate validation is ignored.

By default, time is checked in PKI certificate authentication.

NOTE

Only AR100&AR120&AR150 series, AR161, AR161W, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169G-L, AR169CVW, AR169CVW-4B4S among the AR160 series support this command.

**----End**

### 16.7.5.3 Verifying the CA and Local Certificate Configuration

## Prerequisites

Configuring the validity check for the CA and local certificates has been completed.

## Procedure

- Run the **display pki realm** [ *realm-name* ] command to check the PKI realm configuration.
- Run the **display pki crl** { **realm** *realm-name* | **filename** *filename* } command to check the CRL in the device.
- Run the **display pki certificate ocsp realm** *realm-name* command to check the OCSP server certificate loaded to the device.
- Run the **display pki ocsp cache statistics** command to check the OCSP response cache information.
- Run the **display pki ocsp server down-information** command to check the OCSP server Down records.
- Run the **display ldap-server template** [ *template-name* ] command to check the configurations of the LDAP server template.

**----End**

# 16.7.6 Deleting the Local Certificate

## Context

When a local certificate expires or you want to request a new certificate, delete the existing local certificate.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **pki delete-certificate local realm** *realm-name*

The local certificate is deleted from the memory.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

# 16.7.7 Configuring the Extended Functions

## 16.7.7.1 Configuring Certificate Obtaining

### Context

When the SCEP method is used, the PKI entity queries and obtains issued certificates on the CA server and stores the certificates to the local storage. The PKI entity can download their own certificates, CA certificates, or local certificates of other entities.

After obtaining a CA certificate, the device automatically imports the certificate to the device memory. After the device obtains a local certificate, you need to import it to the memory manually.

The purposes of obtaining a certificate are as follows:

- Stores certificates to the device storage to improve certificate query efficiency and reduce the times of querying the PKI certificate repository.
- Prepares for certificate authentication.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **pki get-certificate** { **ca** | **local** } **realm** *realm-name*

The certificate is saved to the storage.

If the same certificate exists on the device, delete the existing one; otherwise, the certificate cannot be obtained.

**----End**

## 16.7.7.2 Importing and Releasing a Peer Certificate

### Context

In the digital envelope authentication mode, the device as the data sender must have the receiptant's public key configured. Importing a peer certificate is a method to obtain the public key of a peer entity. This method connects the user identity information to the public key. It has high security and is applicable to large networks.

If the imported peer certificate is not used, release the certificate.

### Procedure

- Import the peer certificate
  a. Run **system-view**

     The system view is displayed.

 Copyright © Huawei Technologies Co., Ltd. 

b. Run **pki import-certificate peer** *peer-name* { { **der** | **pem** | **pkcs12** } **filename** [ *filename* ] | **pem terminal** } or **pki import-certificate peer** *peer-name* **pkcs12 filename** *filename* **password** *password*

The peer certificate is imported to the device memory.

- Release the peer certificate
  a. Run **system-view**

  The system view is displayed.
  b. Run **pki release-certificate peer** { **name** *peer-name* | **all** }

  The peer certificate is released.

**----End**

## Verifying the Configuration

Run the **display pki peer-certificate** { **name** *peer-name* | **all** } command to check the imported peer certificate.

## 16.7.7.3 Configuring a Self-Signed Certificate or Local Certificate

## Context

If a device fails to request a local certificate from the CA, it can generate a self-signed certificate or local certificate. The generated certificate is saved in storage as a file and issued to a PKI entity. You can export the certificate and transfer it to another device.

- A self-signed certificate is issued by a device to itself. Therefore, the issuer and subject of a self-signed certificate are identical.
- A local certificate is issued by a device to itself according to the certificate issued by the CA. Therefore, the issuer of a local certificate is the CA.

NOTE

A device does not support lifecycle management (such as certificate update and revocation) over its self-signed certificate. To ensure security of the device and certificate, you are advised to replace the self-signed certificate with the local certificate.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **pki create-certificate** [ **self-signed** ] **filename** *file-name*

A self-signed certificate or local certificate is created.

During the configuration, you will be prompted to enter the certificate information, such as PKI entity attributes, the certificate file name, the certificate validity period, and length of the RSA key pair.

Specify the **self-signed** parameter to create a self-signed certificate. If this parameter is not specified, a local certificate is created.

 Copyright © Huawei Technologies Co., Ltd. 

The file format of the created self-signed certificate or local certificate is PEM.

**----End**

### 16.7.7.4 Adding a PKI to a Specified VPN

#### Context

A device needs to communicate with the CA server to obtain and verify certificates. When the server is in a VPN, add a PKI realm to the VPN.

#### Procedure

1. Run **system-view**

   The system view is displayed.
2. Run **pki realm** *realm-name*

   A PKI realm is created and the PKI realm view is displayed; or the PKI realm view is displayed directly.

   By default, the device has a PKI realm named **default**. This realm can only be modified but cannot be deleted.

   A PKI realm is valid only on the local device and unavailable to certificate authorities (CAs) or other devices. Each PKI realm has its own parameters.
3. Run **vpn-instance** *vpn-instance-name*

   A PKI is added to a specified VPN.

   By default, a PKI does not belong to any VPN.

   The *vpn-instance-name* parameter is set by using the **ip vpn-instance** command.

## 16.8 Maintaining PKI

### 16.8.1 Checking PKI Information

#### Context

During routine maintenance, you can view PKI information in the corresponding view, including information about certificate.

#### Procedure

- Run the **display pki certificate enroll-status** [ **realm** *realm-name* ] command to check the certificate enrollment status.
- Run the **display pki cmp statistics** [ **session** *session-name* ] command to check CMP session statistics.
- Run the **display pki ocsp cache statistics** command to check statistics about the OCSP response cache.
- Run the **display pki ocsp server down-information** command to check the OCSP server Down records.

 Copyright © Huawei Technologies Co., Ltd. 

- Run the **display pki certificate** { **ca** | **local** | **ocsp** } **realm** *realm-name* command to check the content of CA, local, or OCSP server certificate loaded on the device.
- Run the **display pki certificate default** { **ca** | **local** } command to check the default CA certificate and local certificate.
- Run the **display pki peer-certificate** { **name** *peer-name* | **all** } command to check the imported peer certificates.
- Run the **display pki ocsp cache detail** command to check the detail information of the OCSP cache.

**----End**

## 16.8.2 Clearing PKI Information

### Context

Statistics cannot be restored after being cleared. Exercise caution when you run the reset commands.

### Procedure

- Run the **reset pki cmp statistics** [ **session** *session-name* ] command to clear CMP session statistics.
- Run the **reset pki ocsp response cache** command to clear the OCSP response cache.
- Run the **reset pki ocsp server down-information** [ **url** [ **esc** ] *url-addr* ] command to clear the OCSP server Down records.

**----End**

# 16.9 Configuration Examples for PKI

## 16.9.1 Example for Configuring Automatic Local Certificate Application Using SCEP

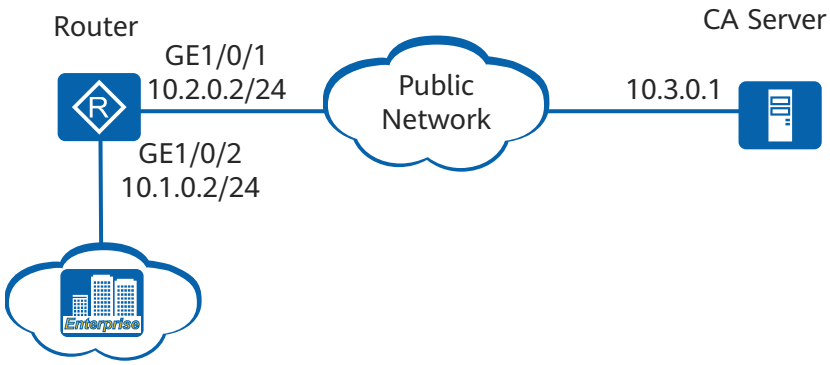
### Networking Requirements

On an enterprise network shown in **Figure 16-11**, the Router is located at the edge to function as the egress gateway and a CA server is located on the public network. The network administrator manually applies for a local certificate from the CA server in online mode.

The network administrator wants to use a simple and fast method to apply for a local certificate, and the certificate can be automatically imported to the memory. In addition, the certificate needs to be automatically updated before expiration. The automatic certificate application through SCEP can be configured to meet these requirements.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 16-11** Automatic local certificate application using SCEP




NOTE

This example provides only the configurations on Router. For the configurations on the CA server, see the CA server product manual. In this example, the CA server runs Windows Server 2008 with the built-in **Certification Services** and with the SCEP plugin installed.

## Configuration Roadmap

The configuration roadmap is as follows:

1. Assign IP addresses to interfaces and static routes to the CA server so that the Router and CA server can communicate with each other.
2. Create an RSA key pair so that the local certificate application request contains the public key.
3. Configure the PKI entity and related information to identify the PKI entity.
4. Configure certificate application through SCEP and automatic certificate update, automatic certificate installation, and automatic certificate update.

## Data Preparation

Obtain the fingerprint and challenge password from the CA server in offline mode. In this example, the digital fingerprint is **e71add0744360e91186b828412d279e06dcc15a4ab4bb3d13842820396b526a0** and challenge password is **6AE73F21E6D3571D**.

For example, from a CA server running Windows Server 2008, you can obtain the digital fingerprint at http://*host*:*port*/certsrv/mscep_admin/, in which *host* indicates the server's IP address and *port* indicates the port number.

## Procedure

**Step 1** Assign IP addresses to interfaces and configure static routes to the CA server.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 10.2.0.2 255.255.255.0
[Router-GigabitEthernet1/0/1] quit
[Router] interface gigabitethernet 1/0/2
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router-GigabitEthernet1/0/2] ip address 10.1.0.2 255.255.255.0
[Router-GigabitEthernet1/0/2] quit
[Router] ip route-static 10.3.0.0 255.255.255.0 10.2.0.1
```

**Step 2** Create an RSA key pair.

# Create a 2048-bit RSA key pair named **rsa_scep** and allow it to be exported.

```
[Router] pki rsa local-key-pair create rsa_scep exportable
 Info: The name of the new key-pair will be: rsa_scep
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...       ..................+++
.....................+++
```

**Step 3** Configure a PKI entity to identify a certificate applicant.

# Configure the PKI entity **user01**.

```
[Router] pki entity user01
[Router-pki-entity-user01] common-name hello
[Router-pki-entity-user01] country cn
[Router-pki-entity-user01] email user@test.abc.com
[Router-pki-entity-user01] fqdn test.abc.com
[Router-pki-entity-user01] ip-address 10.2.0.2
[Router-pki-entity-user01] state jiangsu
[Router-pki-entity-user01] organization huawei
[Router-pki-entity-user01] organization-unit info
[Router-pki-entity-user01] quit
```

**Step 4** Apply for and update the certificate using SCEP.

```
[Router] pki realm abc
[Router-pki-realm-abc] ca id ca_root
[Router-pki-realm-abc] entity user01
[Router-pki-realm-abc] fingerprint sha256
e71add0744360e91186b828412d279e06dcc15a4ab4bb3d13842820396b526a0
[Router-pki-realm-abc] enrollment-url http://10.3.0.1:80/certsrv/mscep/mscep.dll ra
[Router-pki-realm-abc] rsa local-key-pair rsa_scep
[Router-pki-realm-abc] enrollment-request signature message-digest-method sha-384
[Router-pki-realm-abc] password cipher 6AE73F21E6D3571D
```

**Step 5** Enable automatic certificate enrollment and configure the certificate to be updated when 60% of the validity period is passed and the RSA key pair is updated together with the certificate.

```
[Router-pki-realm-abc] auto-enroll 60 regenerate 2048
[Router-pki-realm-abc] quit
```

Before obtaining and installing a local certificate, the device obtains and installs a CA certificate first. The CA and local certificates are named **abc_ca.cer** and **abc_local.cer**.

**Step 6** Verify the configuration.

1. After a local certificate is obtained and imported to memory, run the **display pki certificate local** command to view content of the certificate.

```
[Router] display  pki certificate local realm abc
 The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            48:65:aa:2a:00:00:00:00:3f:c6
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=ca_root
        Validity
            Not Before: Dec 21 11:46:10 2015 GMT
            Not After : Dec 21 11:56:10 2016 GMT
```

 Copyright © Huawei Technologies Co., Ltd. 

```
      Subject: C=CN, ST=jiangsu, O=huawei, OU=info, CN=hello
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
               00:94:6f:49:bd:6a:f3:d5:07:ee:10:ee:4f:d3:06:
               80:59:15:cb:a8:0a:b2:ba:c2:db:52:ec:e9:d1:a7:
               72:de:ac:35:df:bb:e0:72:62:08:3e:c5:54:c1:ba:
               4a:bb:1b:a9:d9:dc:e4:b6:4d:ca:b3:54:90:b6:8e:
               15:a3:6e:2d:b2:9e:9e:7a:33:b0:56:3f:ec:bc:67:
               1c:4c:59:c6:67:0f:a7:03:52:44:8c:53:72:42:bd:
               6e:0c:90:5b:88:9b:2c:95:f7:b8:89:d1:c2:37:3e:
               93:78:fa:cb:2c:20:22:5f:e5:9c:61:23:7b:c0:e9:
               fe:b7:e6:9c:a1:49:0b:99:ef:16:23:e9:44:40:6d:
               94:79:20:58:d7:e1:51:a1:a6:4b:67:44:f7:07:71:
               54:93:4e:32:ff:98:b4:2b:fa:5d:b2:3c:5b:df:3e:
               23:b2:8a:1a:75:7e:8f:82:58:66:be:b3:3c:4a:1c:
               2c:64:d0:3f:47:13:d0:5a:29:94:e2:97:dc:f2:d1:
               06:c9:7e:54:b3:42:2e:15:b8:40:f3:94:d3:76:a1:
               91:66:dd:40:29:c3:69:70:6d:5a:b7:6b:91:87:e8:
               bb:cb:a5:7e:ec:a5:31:11:f3:04:ab:1a:ef:10:e6:
               f1:bd:d9:76:42:6c:2e:bf:d9:91:39:1d:08:d7:b4:
               18:53
            Exponent: 65537 (0x10001)
      X509v3 extensions:
         X509v3 Subject Alternative Name:
            IP Address:10.2.0.2, DNS:test.abc.com, email:user@test.abc.com
         X509v3 Subject Key Identifier:
            15:D1:F6:24:EB:6B:C0:26:19:58:88:91:8B:60:42:CE:BA:D5:4D:F3
         X509v3 Authority Key Identifier:
            keyid:B8:63:72:A4:5E:19:F3:B1:1D:71:E1:37:26:E1:46:39:01:B6:82:C
5

         X509v3 CRL Distribution Points:

            Full Name:
              URI:file://\\vasp-e6000-127.china.huawei.com\CertEnroll\ca_roo
t.crl
              URI:http://10.3.0.1:8080/certenroll/ca_root.crl

         Authority Information Access:
            CA Issuers - URI:http://vasp-e6000-127.china.huawei.com/CertEnro
ll/vasp-e6000-127.china.huawei.com_ca_root.crt
            OCSP - URI:file://\\vasp-e6000-127.china.huawei.com\CertEnroll\v
asp-e6000-127.china.huawei.com_ca_root.crt

         1.3.6.1.4.1.311.20.2:
            .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
   Signature Algorithm: sha1WithRSAEncryption
      d2:be:a8:52:6b:03:ce:89:f1:5b:49:d4:eb:2b:9f:fd:59:17:
      d4:3c:f1:db:4f:1b:d1:12:ac:bf:ae:59:b4:13:1b:8a:20:d0:
      52:6a:f8:a6:03:a6:72:06:41:d2:a7:7d:3f:51:64:9b:84:64:
      cf:ec:4c:23:0a:f1:57:41:53:eb:f6:3a:44:92:f3:ec:bd:09:
      75:db:02:42:ab:89:fa:c4:cd:cb:09:bf:83:1d:de:d5:4b:68:
      8a:a6:5f:7a:e8:b3:34:d3:e8:ec:24:37:2b:bd:3d:09:ed:88:
      d8:ed:a7:f8:66:aa:6f:b0:fe:44:92:d4:c9:29:21:1c:b3:7a:
      65:51:32:50:5a:90:fa:ae:e1:19:5f:c8:63:8d:a8:e7:c6:89:
      2e:6d:c8:5b:2c:0c:cd:41:48:bd:79:74:0e:b8:2f:48:69:df:
      02:89:bb:b3:59:91:7f:6b:46:29:7e:22:05:8c:bb:6a:7e:f3:
      11:5a:5f:fb:65:51:7d:35:ff:49:9e:ec:d1:2d:7e:73:e5:99:
      c6:41:84:0c:50:11:ed:97:ed:15:de:11:22:73:a1:78:11:2e:
      34:e6:f5:de:66:0c:ba:d5:32:af:b8:54:26:4f:5b:9e:89:89:
      2a:3f:b8:96:27:00:c3:08:3a:e9:e8:a6:ce:4b:5a:e3:97:9e:
      6b:dd:f0:72

Pki realm name: abc
Certificate file name: abc_local.cer
Certificate peer name: -
```

 Copyright © Huawei Technologies Co., Ltd. 

2. After a CA certificate is obtained and imported to memory, run the **display pki certificate ca** command to view content of the certificate.

```
[Router] display  pki certificate ca realm abc
 The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0c:f0:1a:f3:67:21:44:9a:4a:eb:ec:63:75:5d:d7:5f
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=ca_root
        Validity
            Not Before: Jun  4 14:58:17 2015 GMT
            Not After : Jun  4 15:07:10 2020 GMT
        Subject: CN=ca_root
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d9:5f:2a:93:cb:66:18:59:8c:26:80:db:cd:73:
                    d5:68:92:1b:04:9d:cf:33:a2:73:64:3e:5f:fe:1a:
                    53:78:0e:3d:e1:99:14:aa:86:9b:c3:b8:33:ab:bb:
                    76:e9:82:f6:8f:05:cf:f6:83:8e:76:ca:ff:7d:f1:
                    bc:22:74:5e:8f:4c:22:05:78:d5:d6:48:8d:82:a7:
                    5d:e1:4c:a4:a9:98:ec:26:a1:21:07:42:e4:32:43:
                    ff:b6:a4:bd:5e:4d:df:8d:02:49:5d:aa:cc:62:6c:
                    34:ab:14:b0:f1:58:4a:40:20:ce:be:a5:7b:77:ce:
                    a4:1d:52:14:11:fe:2a:d0:ac:ac:16:95:78:34:34:
                    21:36:f2:c7:66:2a:14:31:28:dc:7f:7e:10:12:e5:
                    6b:29:9a:e8:fb:73:b1:62:aa:7e:bd:05:e5:c6:78:
                    6d:3c:08:4c:9c:3f:3b:e0:e9:f2:fd:cb:9a:d1:b7:
                    de:1e:84:f4:4a:7d:e2:ac:08:15:09:cb:ee:82:4b:
                    6b:bd:c6:68:da:7e:c8:29:78:13:26:e0:3c:6c:72:
                    39:c5:f8:ad:99:e4:c3:dd:16:b5:2d:7f:17:e4:fd:
                    e4:51:7a:e6:86:f0:e7:82:2f:55:d1:6f:08:cb:de:
                    84:da:ce:ef:b3:b1:d6:b3:c0:56:50:d5:76:4d:c7:
                    fb:75
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.20.2:
                ...C.A
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                B8:63:72:A4:5E:19:F3:B1:1D:71:E1:37:26:E1:46:39:01:B6:82:C5
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://vasp-e6000-127.china.huawei.com/CertEnroll/ca_root.
crl
                  URI:file://\\vasp-e6000-127.china.huawei.com\CertEnroll\ca_roo
t.crl

            1.3.6.1.4.1.311.21.1:
                ...
    Signature Algorithm: sha1WithRSAEncryption
        52:21:46:b8:67:c8:c3:4a:e7:f8:cd:e1:02:d4:24:a7:ce:50:
        be:33:af:8a:49:47:67:43:f9:7f:79:88:9c:99:f5:87:c9:ff:
        08:0f:f3:3b:de:f9:19:48:e5:43:0e:73:c7:0f:ef:96:ef:5a:
        5f:44:76:02:43:83:95:c4:4e:06:5e:11:27:69:65:97:90:4f:
        04:4a:1e:12:37:30:95:24:75:c6:a4:73:ee:9d:c2:de:ea:e9:
        05:c0:a4:fb:39:ec:5c:13:29:69:78:33:ed:d0:18:37:6e:99:
        bc:45:0e:a3:95:e9:2c:d8:50:fd:ca:c2:b3:5a:d8:45:82:6e:
        ec:cc:12:a2:35:f2:43:a5:ca:48:61:93:b9:6e:fe:7c:ac:41:
        bf:88:70:57:fc:bb:66:29:ae:73:9c:95:b9:bb:1d:16:f7:b4:
        6a:da:03:df:56:cf:c7:c7:8c:a9:19:23:61:5b:66:22:6f:7e:
        1d:26:92:69:53:c8:c6:0e:b3:00:ff:54:77:5e:8a:b5:07:54:
```

 Copyright © Huawei Technologies Co., Ltd. 

```
      fd:18:39:0a:03:ac:1d:9f:1f:a1:eb:b9:f8:0d:21:25:36:d5:
      06:de:33:fa:7b:c8:e9:60:f3:76:83:bf:63:c6:dc:c1:2c:e4:
      58:b9:cb:48:15:d2:a8:fa:42:72:15:43:ef:55:63:39:58:77:
      e8:ae:0f:34

Pki realm name: abc
Certificate file name: abc_ca.cer
Certificate peer name: -
```

3. When 60% of the certificate validity period has elapsed, the device sends a certificate update request to the SCEP server.

   The **regenerate** parameter has been specified for **auto-enroll**, so the device generates a new RSA key pair to apply for a new certificate.

**----End**

## Configuration Files

Router configuration file

```
#
sysname Router
#
pki entity user01
 country CN
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
 fqdn test.abc.com
 ip-address 10.2.0.2
 email user@test.abc.com
#
pki realm abc
 ca id ca_root
 enrollment-url http://10.3.0.1:80/certsrv/mscep/mscep.dll ra
 entity user01
 fingerprint sha256 e71add0744360e91186b828412d279e06dcc15a4ab4bb3d13842820396b526a0
 rsa local-key-pair rsa_scep
 password cipher %^%#\c{UCn\RwO'<$oTEf1Q%rZp"U$(K{GGPvZN(qw,B%^%#
 auto-enroll 60 regenerate
 enrollment-request signature message-digest-method sha-384
#
interface GigabitEthernet1/0/1
 ip address 10.2.0.2 255.255.255.0
interface GigabitEthernet1/0/2
 ip address 10.1.0.2 255.255.255.0
#
ip route-static 10.3.0.0 255.255.255.0 10.2.0.1
#
return
```

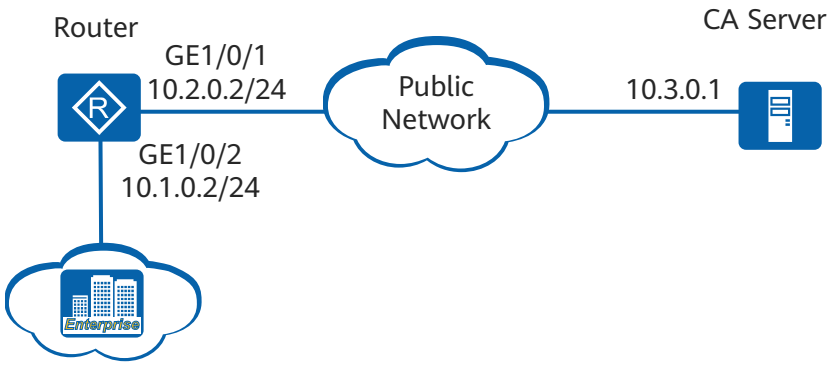
# 16.9.2 Example for Configuring Initial Application of Local Certificate Using CMPv2

## Networking Requirements

On an enterprise network shown in **Figure 16-12**, the Router is located at the edge to function as the egress gateway. The Router uses CMPv2 to apply for a local certificate for the first time from the CA server located on the public network. The local certificate will be automatically downloaded to the device storage.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 16-12** Initial application of local certificate application using CMPv2




NOTE

This example provides only the configurations on Router. For the configurations on the CA server, see the CA server product manual.

Only HTTP+CMPv2 can be used to apply for certificates. HTTPS+CMPv2 is not supported.

## Configuration Roadmap

The configuration roadmap is as follows:

1. Assign IP addresses to interfaces and static routes to the CA server so that the Router and CA server can communicate with each other.
2. Create an RSA key pair so that the local certificate application request contains the public key.
3. Configure the PKI entity and related information to identify the pki entity.
4. Configure certificate application and automatic update using CMPv2 and use the MAC to authenticate messages so that the device can automatically download the CA and local certificates.
5. Install the CA and local certificates to make the certificates effective. That is, the device can use the certificates to protect communication data.

## Data Preparation

To complete the configuration, you need the following data:

- CA name

  Subject of the CA certificate
- Reference and secret values of the MAC

  Obtained from the CMP server in out-of-band mode.

## Procedure

**Step 1** Assign IP addresses to interfaces and configure static routes to the CA server.

```
<Huawei> system-view
[Huawei] sysname Router
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 10.2.0.2 255.255.255.0
[Router-GigabitEthernet1/0/1] quit
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip address 10.1.0.2 255.255.255.0
[Router-GigabitEthernet1/0/2] quit
[Router] ip route-static 10.3.0.0 255.255.255.0 10.2.0.1
```

**Step 2** Create an RSA key pair.

# Create a 2048-bit RSA key pair named **rsa_cmp** and allow it to be exported.

```
[Router] pki rsa local-key-pair create rsa_cmp exportable
 Info: The name of the new key-pair will be: rsa_cmp
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
.....+++
.....+++
```

**Step 3** Configure a PKI entity to identify the certificate applicant.

# Configure the PKI entity **user01**.

```
[Router] pki entity user01
[Router-pki-entity-user01] common-name hello
[Router-pki-entity-user01] country cn
[Router-pki-entity-user01] email user@test.abc.com
[Router-pki-entity-user01] fqdn test.abc.com
[Router-pki-entity-user01] ip-address 10.2.0.2
[Router-pki-entity-user01] state jiangsu
[Router-pki-entity-user01] organization huawei
[Router-pki-entity-user01] organization-unit info
[Router-pki-entity-user01] quit
```

**Step 4** Configure the PKI realm.

```
[Router] pki realm abc
[Router-pki-realm-abc] quit
```

**Step 5** Configure the CMP session.

# Create the CMP session named **cmp**.

```
[Router] pki cmp session cmp
```

# Specify the pki entity name referenced by the CMP session.

```
[Router-pki-cmp-session-cmp] cmp-request entity user01
```

# Configure a CA name, for example, C=cn,ST=beijing,L=SD,O=BB,OU=BB,CN=BB.

**NOTE**

The field order in the CA name must be the same as that in the CA certificate; otherwise, the server considers the CA name invalid.

```
[Router-pki-cmp-session-cmp] cmp-request ca-name "C=cn,ST=beijing,L=SD,O=BB,OU=BB,CN=BB"
```

# Configure the URL for certificate application.

```
[Router-pki-cmp-session-cmp] cmp-request server url http://10.3.0.1:8080
```

# Specify the RSA key pair used for certificate application and configure the device to update the RSA key pair together with the certificate.

```
[Router-pki-cmp-session-cmp] cmp-request rsa local-key-pair rsa_cmp regenerate
```

# Specify a PKI domain to which the CMP server certificate belongs. Set a PKI domain name of the CMP server certificate to **abc**.

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router-pki-cmp-session-cmp] cmp-request realm abc
```

# Use the MAC for initial certificate application. Set the MAC reference value to 1234 and secret value to 123456.

```
[Router-pki-cmp-session-cmp] cmp-request message-authentication-code 1234 123456
[Router-pki-cmp-session-cmp] quit
[Router] pki cmp initial-request session cmp
[Router]
 Info: Initializing configuration.
 Info: Creatting initial request packet.
 Info: Connectting to CMPv2 server.
 Info: Sending initial request packet.
 Info: Waitting for initial response packet.
 Info: Creatting confirm packet.
 Info: Connectting to CMPv2 server.
 Info: Sending confirm packet.
 Info: Waitting for confirm packet from server.
 Info: CMPv2 operation finish.
```

The CA and local certificates are named **cmp_ca1.cer** and **cmp_ir.cer** and stored in the device storage.

**Step 6** Install the certificates.

# Import the CA certificate to the PKI realm.

```
[Router] pki import-certificate ca realm abc pem filename cmp_ca1.cer
 The CA's Subject is /C=cn/ST=beijing/L=BB/O=BB/OU=BB/CN=BB
 The CA's fingerprint is:
   MD5  fingerprint:3AC7 54FD E272 09BE 9008 84EE D1FC 118E
   SHA1 fingerprint:492A 8E0B BED2 BE10 C097 9039 99FE F7E1 9AA5 B658
 Is the fingerprint correct?(Y/N):y
 Info: Succeeded in importing file.
```

# Import the local certificate to the PKI realm.

```
[Router] pki import-certificate local realm abc pem filename cmp_ir.cer
 Info: Succeeded in importing file.
```

**Step 7** Configure automatic certificate update.

# Configure the certificate that proves the device itself, which is the certificate to be updated, **cmp_ir.cer**.

```
[Router] pki cmp session cmp
[Router-pki-cmp-session-cmp] cmp-request authentication-cert cmp_ir.cer
```

# Enable automatic certificate update.

```
[Router-pki-cmp-session-cmp] certificate auto-update enable
```

# Configure the device to update the certificate when 60% of the certificate validity period has elapsed.

```
[Router-pki-cmp-session-cmp] certificate update expire-time 60
[Router-pki-cmp-session-cmp] quit
```

**Step 8** Verify the configuration.

1. After a local certificate is obtained and imported to memory, run the **display pki certificate** command to view content of the certificate.

```
[Router] display pki certificate filename cmp_ir.cer
 The  x509_obj type is Cert:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1144733510 (0x443b3f46)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, ST=beijing, L=BB, O=BB, OU=BB, CN=BB
```

 Copyright © Huawei Technologies Co., Ltd. 

```
    Validity
        Not Before: Jun 12 09:33:10 2012 GMT
        Not After : Aug 13 02:38:27 2016 GMT
    Subject: C=CN, ST=jiangsu, O=huawei, OU=info, CN=hello
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:d3:12:fe:57:48:c6:a5:10:12:e9:2f:f9:2a:ff:
                7b:2a:d8:45:69:11:c4:85:30:c4:9a:4d:0f:ad:58:
                e7:56:cd:5c:f0:18:e1:c3:6d:44:c2:c3:5e:64:22:
                d1:28:c9:c3:37:3c:34:ed:28:04:7f:62:9e:8b:94:
                af:bc:72:de:f6:72:7f:e4:d8:45:31:fd:f9:ac:ce:
                5a:b9:c7:1b:23:53:00:28:a6:3b:f5:61:69:5d:ab:
                67:cb:bb:e8:96:2f:ce:ab:2c:6b:91:5b:26:91:86:
                8f:80:a9:b0:66:c1:16:3d:31:55:a2:d4:b5:5a:af:
                85:88:6e:99:f8:f8:53:58:77:26:91:ed:0e:94:ad:
                c5:8d:53:67:67:55:08:8d:90:38:e0:5e:96:37:b9:
                64:0e:36:e7:cf:9a:d2:77:e4:b0:24:05:a6:eb:03:
                6e:ff:f7:ab:be:93:9e:8c:66:7d:31:66:be:6d:c8:
                f3:17:9d:86:19:88:21:2d:d9:69:86:5f:b2:55:a4:
                db:bc:d7:d0:6b:ac:66:ac:e4:63:9c:66:79:9c:42:
                5c:83:b8:9e:4b:6e:67:85:a2:47:19:f1:5c:c0:3c:
                c9:a3:47:02:a8:53:69:59:9e:d9:c7:5e:90:83:8d:
                ac:cd:21:3c:d5:31:39:49:84:e6:f8:f4:e0:44:dd:
                5d:7b
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Alternative Name:
            IP Address:10.2.0.2, DNS:test.abc.com, email:user@test.abc.com
Signature Algorithm: sha1WithRSAEncryption
    53:d5:79:31:7b:40:52:aa:ec:a9:35:ed:07:62:32:c4:ce:22:
    d3:37:0e:83:0c:4c:fa:61:dd:8c:db:a8:d3:fd:6a:ca:0e:3c:
    91:2c:91:ab:92:31:34:b5:87:1e:30:a4:ff:94:9c:d2:71:3c:
    6b:1f:4f:be:a7:20:f2:e1:c2:ad:71:8b:c2:79:0f:50:1f:3c:
    f9:87:df:1d:ee:3d:38:8c:f3:30:b7:3b:00:9b:72:38:b0:68:
    e1:c0:08:f4:02:91:81:a8:fa:51:9e:53:0d:03:b3:6b:0e:e2:
    62:80:ef:2a:a0:cb:9b:9b:91:21:7c:df:fe:6a:38:cc:03:36:
    9c:fc

Pki realm name: abc
Certificate file name: cmp_ir.cer
Certificate peer name: -
```

2. After a CA certificate is obtained and imported to memory, run the **display pki certificate** command to view content of the certificate.

```
[Router] display pki certificate filename cmp_ca1.cer
 The x509 object  type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, ST=beijing, L=BB, O=BB, OU=BB, CN=BB
        Validity
            Not Before: Aug 15 02:38:27 2011 GMT
            Not After : Aug 13 02:38:27 2016 GMT
        Subject: C=CN, ST=jiangsu, O=huawei, OU=info, CN=hello
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b7:3e:65:7f:3b:3c:18:b8:87:34:39:76:3c:87:
                    39:f7:a9:b3:35:9b:e0:e0:5b:c7:4f:3c:bb:fa:dd:
                    da:93:0b:55:6e:eb:ba:52:c8:86:d1:cf:14:1e:1c:
                    35:c6:53:68:f3:51:e7:2c:d4:b8:fa:0f:b3:04:ef:
                    3f:a0:b3:4d:78:c1:26:88:26:15:41:3d:14:7f:67:
                    3e:2f:35:32:ce:c7:73:73:43:5c:12:d3:0f:a0:ec:
                    96:ae:55:61:27:32:39:a4:f8:32:a1:68:50:e6:3d:
```

 Copyright © Huawei Technologies Co., Ltd. 

```
                2b:39:6d:42:e8:09:5d:4f:98:46:6e:fc:80:87:0e:
                36:ca:09:7a:ca:2f:dd:ad:d3
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                4F:67:F4:CB:F4:C3:F7:61:2C:BD:FF:1D:D1:29:FD:39:28:9F:3B:8B
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            Netscape Cert Type:
                SSL CA, S/MIME CA, Object Signing CA
            Netscape Comment:
                xca certificate
    Signature Algorithm: sha1WithRSAEncryption
        75:43:24:eb:db:ee:7d:05:30:88:b8:1b:d5:32:ca:51:49:74:
        04:94:fe:d0:31:29:6f:72:c7:4a:86:ac:2a:4c:45:24:9d:3c:
        b4:30:b5:d1:43:88:29:f7:b4:88:b8:37:dc:dd:f4:fa:42:34:
        1c:e6:a5:bc:bb:0b:37:ef:db:8c:b2:b0:bd:97:7f:15:ae:6c:
        71:1b:ff:f1:90:13:74:a4:1f:7c:f7:4e:80:5b:42:aa:6b:22:
        2a:cf:04:48:29:20:c0:b2:95:38:11:06:be:76:f0:cb:8d:4a:
        c6:1a:50:af:31:81:58:ac:14:fe:89:f2:e0:bb:95:3c:94:d0:
        54:96

Pki realm name: abc
Certificate file name: cmp_ca1.cer
Certificate peer name: -
```

3. When 60% of the certificate validity period has elapsed, the device sends a certificate update request to the CMPv2 server.

   The **regenerate** parameter has been specified for **cmp-request rsa local-key-pair**, so the device generates a new RSA key pair to apply for a new certificate. The new certificate will replace the certificate files in the device storage and memory.

**----End**

## Configuration Files

Router configuration file

```
#
sysname Router
#
pki entity user01
 country CN
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
 fqdn user@test.abc.com
 ip-address 10.2.0.2
 email user@user@test.abc.com
#
pki realm abc
#
interface Ethernet2/0/0
 ip address 10.2.0.2 255.255.255.0
interface Ethernet1/0/2
 ip address 10.1.0.2 255.255.255.0
#
pki cmp session cmp
 cmp-request ca-name "C=cn,ST=beijing,L=SD,O=BB,OU=BB,CN=BB"
 cmp-request authentication-cert cmp_ir.cer
 cmp-request entity user01
 cmp-request server url http://10.3.0.1:8080
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 cmp-request rsa local-key-pair rsa_cmp regenerate
 cmp-request realm abc
 cmp-request message-authentication-code 1234 %^%#ZodFBGH[^BkU2(~>[NRBv|#b>se|@I7"'A,llG_B%^
%#
 certificate auto-update enable
 certificate update expire-time 60
#
ip route-static 10.3.0.0 255.255.255.0 10.2.0.1
#
return
```

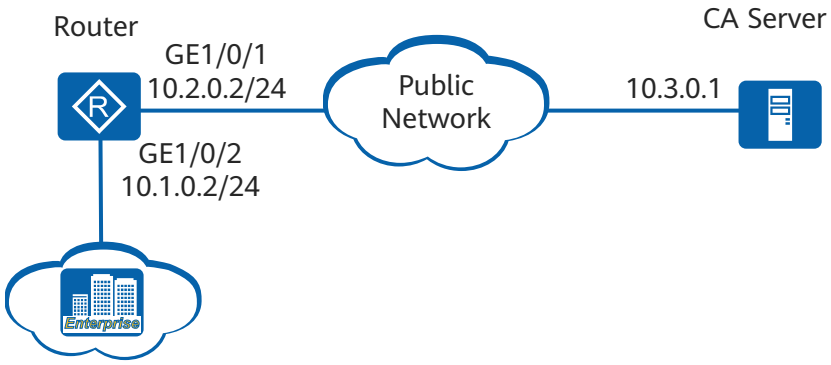
## 16.9.3 Example for Applying for the Local Certificate in Offline Mode

### Networking Requirements

On an enterprise network shown in **Figure 16-13**, the Router is located at the edge to function as the egress gateway and a CA server is located on the public network. The network administrator manually applies for a local certificate from the CA server.

If you fail to apply for a local certificate using SCEP, you can use the offline (out-of-band) mode.

**Figure 16-13** Applying for the local certificate in offline mode




**NOTE**

This example provides only the configurations on Router. For the configurations on the CA server, see the CA server product manual. In this example, the CA server runs Windows Server 2008 with the built-in **Certification Services** and with the SCEP plugin installed.

### Configuration Roadmap

The configuration roadmap is as follows:

1. Create an RSA key pair so that the local certificate application request contains the public key.
2. Configure the PKI entity and related information to identify the PKI entity.
3. Configure offline local certificate application for the PKI entity and generate a local certificate request file.

 Copyright © Huawei Technologies Co., Ltd. 

4. Send the local certificate request file and download the local certificate in out-of-band mode.
5. Install the local certificate so that the device can protect communication data.

## Procedure

**Step 1** Assign IP addresses to interfaces and configure static routes to the CA server.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 10.2.0.2 255.255.255.0
[Router-GigabitEthernet1/0/1] quit
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] ip address 10.1.0.2 255.255.255.0
[Router-GigabitEthernet1/0/2] quit
[Router] ip route-static 10.3.0.0 255.255.255.0 10.2.0.1
```

**Step 2** Create an RSA key pair.

# Create a 2048-bit RSA key pair named **rsa** and allow it to be exported.

```
[Router] pki rsa local-key-pair create rsakey exportable
 Info: The name of the new key-pair will be: rsakey
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...       ..................+++
.....................+++
```

**Step 3** Configure a PKI entity to identify a certificate applicant.

# Configure the PKI entity **user01**.

```
[Router] pki entity user01
[Router-pki-entity-user01] common-name hello
[Router-pki-entity-user01] country cn
[Router-pki-entity-user01] email user@test.abc.com
[Router-pki-entity-user01] fqdn test.abc.com
[Router-pki-entity-user01] ip-address 10.2.0.2
[Router-pki-entity-user01] state jiangsu
[Router-pki-entity-user01] organization huawei
[Router-pki-entity-user01] organization-unit info
[Router-pki-entity-user01] quit
```

**Step 4** Apply for the local certificate in offline mode.

```
[Router] pki realm abc
[Router-pki-realm-abc] entity user01
[Router-pki-realm-abc] rsa local-key-pair rsakey
[Router-pki-realm-abc] quit
[Router] pki enroll-certificate realm abc pkcs10 filename cer_req
 Info: Creating certificate request file...
 Info: Create certificate request file successfully.
```

After the configurations are complete, run the **display pki cert-req** command to view content of the certificate request file.

```
[Router] display pki cert-req filename cer_req
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=CN, ST=jiangsu, O=huawei, OU=info, CN=hello
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a2:db:e3:30:17:8e:f6:2d:2e:64:15:46:51:ad:
                    70:86:dd:32:c4:bb:6b:58:3a:8c:5f:a0:06:a1:e1:
```

 Copyright © Huawei Technologies Co., Ltd. 

```
                56:2e:a4:eb:7e:12:06:05:04:28:b2:6d:64:7a:9c:
                4f:85:24:c1:aa:b8:99:dc:e9:bb:c4:1e:e2:9d:a0:
                18:51:1f:ad:b5:2f:60:18:06:8b:c1:cc:6f:32:58:
                f2:21:2c:16:e8:29:c2:a8:c5:aa:9d:6c:1e:ca:14:
                fc:7a:e9:bc:07:91:ce:ed:a0:c0:52:d9:0c:e9:ba:
                9b:64:43:e0:9a:3f:c5:d1:2c:86:36:96:6b:4b:4f:
                d4:df:05:d0:4b:41:2c:ec:0a:d7:0e:45:83:ed:cd:
                07:78:40:ed:d5:3d:7f:fe:0f:08:90:04:2e:ac:e5:
                42:b9:81:ea:ec:77:e2:cc:04:6e:e4:63:9f:69:ed:
                60:06:5e:c7:e8:bf:30:57:6a:5d:e0:46:68:d3:ee:
                b0:da:47:24:e3:b6:a5:f3:20:d8:5a:75:92:70:c2:
                a9:a6:97:07:07:0d:1c:94:9a:03:6f:f7:8c:db:6f:
                b7:06:de:51:50:9e:71:fd:86:f3:b5:c9:99:05:bf:
                f1:10:20:28:d3:a6:29:3d:e0:f4:a7:ba:1e:27:85:
                a9:66:fc:a9:90:49:f0:35:f7:d9:6d:06:a2:43:3f:
                18:87
            Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Subject Alternative Name:
                IP Address:10.2.0.2, DNS:test.abc.com, email:user@test.abc.com
    Signature Algorithm: sha256WithRSAEncryption
        0e:0a:a5:b7:d5:54:11:10:c4:ea:ff:77:da:f9:24:4b:a9:98:
        a1:75:36:08:10:59:60:fa:1a:30:70:2c:b7:f6:5f:5e:31:b7:
        55:a5:7a:26:e5:af:4a:cd:83:c5:f3:90:f3:b9:d5:f9:0a:6d:
        6e:8f:25:b4:ed:95:9c:75:a5:d7:b6:25:fc:8d:39:89:fb:af:
        37:fc:01:7b:09:07:9c:96:7c:fa:28:6d:e2:11:49:a7:95:94:
        ed:26:5b:ca:f8:98:b0:e7:64:7e:dd:2d:75:ff:89:03:b7:0a:
        92:53:25:d4:a1:23:b9:5c:eb:5b:29:1d:8a:92:8f:36:68:7b:
        77:32:bc:48:92:48:84:fa:87:5a:d7:2e:3e:be:d5:6b:e4:df:
        b1:f2:02:35:91:6a:eb:cd:fc:5a:ea:37:85:6c:12:74:5f:a5:
        5c:c0:05:09:cd:34:59:0d:c6:c8:75:ca:1c:18:d6:48:e5:4b:
        e7:8e:e3:ff:25:99:0f:2e:a8:b4:c5:8e:4d:8f:dd:64:c5:1f:
        61:3c:58:21:4f:d5:35:ba:c8:8e:5f:76:41:9f:27:41:0a:94:
        59:2c:59:25:2d:de:60:5c:92:07:ac:8a:a5:7a:ba:75:af:2c:
        82:5f:bb:55:a8:48:49:54:0f:99:54:af:8d:12:4d:4b:7d:8b:
        95:28:ce:dc
```

**Step 5** Transfer the certificate request file to the CA server in out-of-band mode, for example, web, disk, and email, to apply for a local certificate.

When the local certificate is successfully registered, download the local certificate abc_local.cer also in out-of-band mode. Transfer the certificate file to the device storage using a file transfer protocol.

**Step 6** Install the local certificate.

```
[Router] pki import-certificate local realm abc pem filename abc_local.cer
 Info: Succeeded in importing file.
```

Install the local certificate so that the device can protect communication data.

**Step 7** Verify the configuration.

Run the **display pki certificate local** command to view the content of the local certificate imported to memory.

```
[Router] display  pki certificate local realm abc
 The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            48:65:aa:2a:00:00:00:00:3f:c6
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=ca_root
        Validity
            Not Before: Dec 21 11:46:10 2015 GMT
            Not After : Dec 21 11:56:10 2016 GMT
```

 Copyright © Huawei Technologies Co., Ltd. 

```
      Subject: C=CN, ST=jiangsu, O=huawei, OU=info, CN=hello
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
               00:94:6f:49:bd:6a:f3:d5:07:ee:10:ee:4f:d3:06:
               80:59:15:cb:a8:0a:b2:ba:c2:db:52:ec:e9:d1:a7:
               72:de:ac:35:df:bb:e0:72:62:08:3e:c5:54:c1:ba:
               4a:bb:1b:a9:d9:dc:e4:b6:4d:ca:b3:54:90:b6:8e:
               15:a3:6e:2d:b2:9e:9e:7a:33:b0:56:3f:ec:bc:67:
               1c:4c:59:c6:67:0f:a7:03:52:44:8c:53:72:42:bd:
               6e:0c:90:5b:88:9b:2c:95:f7:b8:89:d1:c2:37:3e:
               93:78:fa:cb:2c:20:22:5f:e5:9c:61:23:7b:c0:e9:
               fe:b7:e6:9c:a1:49:0b:99:ef:16:23:e9:44:40:6d:
               94:79:20:58:d7:e1:51:a1:a6:4b:67:44:f7:07:71:
               54:93:4e:32:ff:98:b4:2b:fa:5d:b2:3c:5b:df:3e:
               23:b2:8a:1a:75:7e:8f:82:58:66:be:b3:3c:4a:1c:
               2c:64:d0:3f:47:13:d0:5a:29:94:e2:97:dc:f2:d1:
               06:c9:7e:54:b3:42:2e:15:b8:40:f3:94:d3:76:a1:
               91:66:dd:40:29:c3:69:70:6d:5a:b7:6b:91:87:e8:
               bb:cb:a5:7e:ec:a5:31:11:f3:04:ab:1a:ef:10:e6:
               f1:bd:d9:76:42:6c:2e:bf:d9:91:39:1d:08:d7:b4:
               18:53
            Exponent: 65537 (0x10001)
      X509v3 extensions:
         X509v3 Subject Alternative Name:
            IP Address:10.2.0.2, DNS:test.abc.com, email:user@test.abc.com
         X509v3 Subject Key Identifier:
            15:D1:F6:24:EB:6B:C0:26:19:58:88:91:8B:60:42:CE:BA:D5:4D:F3
         X509v3 Authority Key Identifier:
            keyid:B8:63:72:A4:5E:19:F3:B1:1D:71:E1:37:26:E1:46:39:01:B6:82:C
5

         X509v3 CRL Distribution Points:

            Full Name:
              URI:file://\\vasp-e6000-127.china.huawei.com\CertEnroll\ca_roo
t.crl
              URI:http://10.3.0.1:8080/certenroll/ca_root.crl

         Authority Information Access:
            CA Issuers - URI:http://vasp-e6000-127.china.huawei.com/CertEnro
ll/vasp-e6000-127.china.huawei.com_ca_root.crt
            OCSP - URI:file://\\vasp-e6000-127.china.huawei.com\CertEnroll\v
asp-e6000-127.china.huawei.com_ca_root.crt

         1.3.6.1.4.1.311.20.2:
            .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
   Signature Algorithm: sha1WithRSAEncryption
      d2:be:a8:52:6b:03:ce:89:f1:5b:49:d4:eb:2b:9f:fd:59:17:
      d4:3c:f1:db:4f:1b:d1:12:ac:bf:ae:59:b4:13:1b:8a:20:d0:
      52:6a:f8:a6:03:a6:72:06:41:d2:a7:7d:3f:51:64:9b:84:64:
      cf:ec:4c:23:0a:f1:57:41:53:eb:f6:3a:44:92:f3:ec:bd:09:
      75:db:02:42:ab:89:fa:c4:cd:cb:09:bf:83:1d:de:d5:4b:68:
      8a:a6:5f:7a:e8:b3:34:d3:e8:ec:24:37:2b:bd:3d:09:ed:88:
      d8:ed:a7:f8:66:aa:6f:b0:fe:44:92:d4:c9:29:21:1c:b3:7a:
      65:51:32:50:5a:90:fa:ae:e1:19:5f:c8:63:8d:a8:e7:c6:89:
      2e:6d:c8:5b:2c:0c:cd:41:48:bd:79:74:0e:b8:2f:48:69:df:
      02:89:bb:b3:59:91:7f:6b:46:29:7e:22:05:8c:bb:6a:7e:f3:
      11:5a:5f:fb:65:51:7d:35:ff:49:9e:ec:d1:2d:7e:73:e5:99:
      c6:41:84:0c:50:11:ed:97:ed:15:de:11:22:73:a1:78:11:2e:
      34:e6:f5:de:66:0c:ba:d5:32:af:b8:54:26:4f:5b:9e:89:89:
      2a:3f:b8:96:27:00:c3:08:3a:e9:e8:a6:ce:4b:5a:e3:97:9e:
      6b:dd:f0:72

Pki realm name: abc
```

 Copyright © Huawei Technologies Co., Ltd. 

```
Certificate file name: abc_local.cer
Certificate peer name: -
```

**----End**

### Configuration Files

Router configuration file

```
#
sysname Router
#
pki entity user01
 country CN
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
 fqdn test.abc.com
 ip-address 10.2.0.2
 email user@test.abc.com

#
pki realm abc
 entity user01
 rsa local-key-pair rsakey
#
interface GigabitEthernet1/0/1
 ip address 10.2.0.2 255.255.255.0
interface GigabitEthernet1/0/2
 ip address 10.1.0.2 255.255.255.0
#
ip route-static 10.3.0.0 255.255.255.0 10.2.0.1
#
return
```

## 16.10 Troubleshooting PKI

## 16.10.1 A CA Certificate Failed to Be Obtained

### Fault Symptom

- The network administrator has manually applied for a CA certificate; however, the CA certificate does not exist in the device storage. The reason is that the configuration about downloading CA certificates using HTTP or LDAP is incorrect.
- The administrator applies for a CA certificate using SCEP. However, the CA certificate does not exist in the device storage. The possible causes are as follows:
  - The command for obtaining the CA certificate is not executed.
  - The trusted CA name is incorrect or not configured.
  - The URL of certificate enrollment server is incorrect or not configured.
  - The PKI entity is not configured.
  - The fingerprint is incorrect or not configured.
  - The RSA key pair is not configured.
  - The source interface for TCP connection is incorrect.

 Copyright © Huawei Technologies Co., Ltd. 

### Procedure

- Obtain a CA certificate manually.

  Check whether the configuration about downloading a CA certificate using HTTP or LDAP is correct. If not, modify the configuration using the **pki http** or **pki ldap** command.
- Obtain a CA certificate using SCEP.
  a. Check whether the **pki get-certificate** command has been executed in the system view.

     If not, run the **pki get-certificate** command. You will be promoted if the configuration about CA certificate application is incorrect.
  b. Check whether the CA certificate application configuration is correct in the PKI realm.

     Run the **display pki realm** command in any view or the **display this** command in the PKI realm view.

     The following is a sample of CA certificate application configuration:

```
pki realm test
 ca id ca_server   //Specify the CA trusted by the PKI realm.
 enrollment-url http://10.13.14.15:8080/certsrv/mscep/mscep.dll   //Configure the URL for the certificate enrollment server.
 entity zzz   //Specify the PKI entity.
 fingerprint sha1 7a34d94624b1c1bcbf6d763c4a67035d5b578eaf   //Configure the fingerprint for CA certificate verification. The fingerprint is obtained from the CA server.
 rsa local-key-pair 8   //Specify the RSA key pair.
 source interface Ethernet0/0/2   //Specify the source interface (a Layer 3 interface with IP address assigned) for the TCP connection. By default, source interface of a TCP connection is the egress interface.
```

     Ensure that the configuration is correct. For details, see **16.7.2.1 Applying for and Updating the Local Certificate Through SCEP**.

**----End**

## 16.10.2 A Local Certificate Failed to Be Obtained

### Fault Symptom

- The administrator applies for a local certificate in offline mode. However, the local certificate does not exist in the device storage. The possible causes are as follows:
  - The PKI entity configuration is incorrect.
  - The challenge password is incorrect or not configured.
  - The configuration about downloading the local certificate using HTTP or LDAP is incorrect.
- The administrator applies for a local certificate using SCEP or CMPv2. However, the local certificate does not exist in the device storage. The possible causes are as follows:
  - No CA certificate exists in the PKI realm.
  - The PKI entity is incorrectly configured or not configured.
  - The trusted CA name is incorrect or not configured.
  - The URL of certificate enrollment server is incorrect or not configured.

 Copyright © Huawei Technologies Co., Ltd. 

- The RSA key pair is not configured.
- The source interface for TCP connection is incorrect.
- Digest method used for the signed certificate enrollment request is incorrect.
- The challenge password is incorrect or not configured.
- THe reference and secret values of MAC are incorrect or not configured.
- The certificate for identity verification is incorrectly configured.

## Procedure

- Obtain a local certificate manually.
  a. Check whether the PKI entity is correctly configured.

     To view the configuration of a PKI entity in a PKI realm, run the **display pki entity** command.

     Modify the incorrect configurations, such as country code. For details, see **16.7.1.1 Configuring a PKI Entity**.
  b. Check whether the challenge password is correct.

     Confirm that the CA server requires a challenge password, and ensure that the challenge password configured on the device is the same as that of the CA server. To set the challenge password, run **pki enroll-certificate**.
  c. Check whether the configuration about downloading a CA certificate using HTTP or LDAP is correct.

     If not, modify the configuration using the **pki http** or **pki ldap** command.
- Obtain a local certificate using SCEP or CMPv2.
  a. Check whether the CA certificate has been imported to the device memory.

     To view the CA certificate in memory, run **display pki certificate**.

     If no CA certificate exists, obtain a CA certificate and run **pki import-certificate** to import the certificate to memory.
  b. Check whether the PKI entity is correctly configured.

     To view the configuration of a PKI entity in a PKI realm, run the **display pki entity** command.

     Modify the incorrect configurations, such as country code. For details, see **16.7.1.1 Configuring a PKI Entity**.
  c. Check whether the CA certificate application configuration is correct in the PKI realm or CMP session.

     - PKI realm

       Run the **display pki realm** command in any view or the **display this** command in the PKI realm view.

       The following is a sample of local certificate application configuration:

```
pki realm test
 ca id ca_server   //Specify the CA trusted by the PKI realm.
 enrollment-url http://10.13.14.15:8080/certsrv/mscep/mscep.dll   //Configure the URL for
```

 Copyright © Huawei Technologies Co., Ltd. 

```
the certificate enrollment server.
 entity zzz  //Specify the PKI entity.
 rsa local-key-pair 8  //Specify the RSA key pair.
 password cipher %^%#\1HN-bn(k;^|O85OAtYF3(M4%^%#  //Configure the challenge password for SCEP certificate application, which is the same as that on the CA server.
 source interface gigabitethernet 1/0/2  //Specify the source interface (a Layer 3 interface with IP address assigned) for the TCP connection. By default, source interface of a TCP connection is the egress interface.
 enrollment-request signature message-digest-method sha1  //Configure the digest algorithm used by the signed certificate enrollment request, which is the same as that on the CA server.
```

Ensure that the configuration is correct. For details, see **16.7.2.1 Applying for and Updating the Local Certificate Through SCEP**.

- CMP session

  Run the **display this** command in the CMP session view.

  The following is a sample of CA certificate application configuration:

```
pki cmp session cmp
 cmp-request ca-name "C=cn,ST=beijing,L=SD,O=BB,OU=BB,CN=BB"  //Configure the CA name. The field order in a CA name must be the same as that in the CA certificate.
 cmp-request authentication-cert local.cer  //Configure the identity authentication certificate in the CMPv2 request, which is used for certificate update or certificate application for another device.
 cmp-request entity user01  //Specify the PKI entity.
 cmp-request server url http://10.3.0.1:8080  //Configure the URL for the CMPv2 server.
 cmp-request rsa local-key-pair rsa  regenerate  //Specify the RSA key pair.
 cmp-request message-authentication-code 1234 %^%#ZodFBGH[^BkU2(~>[NRBv|#b>se|@I7"'A,llG_B%^%#  //Configure the reference and secret values for MAC, which must be the same as those on the CA server.
```

  Ensure that the configuration is correct. For details, see **16.7.2.2 Applying for and Updating the Local Certificate Through CMPv2**.

**----End**

# 16.11 FAQ About PKI

## 16.11.1 What Are the Differences Between CA, Local, and Self-Signed Certificates?

The differences between CA, local, and self-signed certificates are described in **Table 16-5**.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 16-5** Certificate types

| Type | Definition | Description |
| --- | --- | --- |
| Self-signed certificate | A self-signed certificate, which is also called root certificate, is issued by an entity to itself. In this certificate, the issuer name and subject name are the same. | If an applicant fails to apply for a local certificate from the CA, it can generate a self-signed certificate. The self-signed certificate issuing process is simple.<br>A device does not support lifecycle management (such as certificate update and revocation) over its self-signed certificate. To ensure security of the device and certificate, you are advised to replace the self-signed certificate with the local certificate. |
| CA certificate | CA's own certificate. If a PKI system does not have a hierarchical CA structure, the CA certificate is the self-signed certificate. If a PKI system has a hierarchical CA structure, the top CA is the root CA, which owns a self-signed certificate. | An applicant trusts a CA by verifying its digital signature. Any applicant can obtain the CA's certificate (including the public key) to verify the local certificate issued by the CA. |
| Local certificate | A certificate issued by a CA to the applicant. | - |
| Local device certificate | A certificate issued by a device to itself according to the certificate issued by the CA. The issuer name in the certificate is the CA server's name. | If an applicant fails to apply for a local certificate from the CA, it can generate a local device certificate. The local device certificate issuing process is simple. |

## 16.11.2 Which Certificate Formats Are Supported?

Three certificate formats are supported, as described in the table.

 Copyright © Huawei Technologies Co., Ltd. 

**Table 16-6** Certificate formats

| Format | Description | Description |
| --- | --- | --- |
| PKCS#12 | Saves certificate files in binary format, including or excluding the private key. The commonly used file name extensions include .P12 and .PFX. | If the file name extension of a certificate is .CER or .CRT, use the Notepad to open this certificate and check the certificate content to differentiate the certificate format.<br>• If the certificate starts with "-----BEGIN CERTIFICATE-----" and ends with "-----END CERTIFICATE-----", the certificate format is PEM.<br>• If the certificate content is displayed as garbled characters, the certificate format is DER. |
| DER | Saves certificate files in binary format, excluding the private key. The commonly used file name extensions include .DER, .CER, and .CRT. | |
| PEM | Saves certificate files in ASCII format, including or excluding the private key. The commonly used file name extensions include .PEM, .CER, and .CRT. | |

## 16.11.3 How Do I Manually Import Certificates and an RSA Key Pair?

NOTE

Three certificate formats are supported: PKCS#12, DER, and PEM. For details, see **16.11.2 Which Certificate Formats Are Supported?**.

You can enable the device to generate a certificate request file (an RSA key pair has been generated on the device) and provide this file to a certificate authority (CA), which issues only a local certificate. You only need to import the CA and local certificates provided by the CA to the device memory, without having to import the RSA key pair.

Before manually replacing the CA and local certificates, ensure that the CA and local certificates are not being used by services and run the **pki delete-certificate** command to delete the certificates. The following example deletes the local certificate.

```
[Huawei] pki delete-certificate local realm abc
```

The following describes the procedure for manually importing certificates and an RAS key pair:

1. Enable the device to send certificate request information to the CA in out-of-band mode (web, disk, or email) to apply for a local certificate.
2. Download the CA certificate, local certificate, and RSA key pair file, and upload them to the device storage media using TFTP.

   Generally, certificates in DER or PEM format and key pairs are in different files, and certificates in PKCS#12 format and key pairs are in the same file.

 Copyright © Huawei Technologies Co., Ltd. 

3. Import the CA certificate. If there are multiple CA certificates, import all CA certificates.

   For example, the obtained CA certificate file is named **rootca.pem**.

   ```
   <Huawei> system-view
   [Huawei] pki realm abc
   [Huawei-pki-realm-abc] quit
   [Huawei] pki import-certificate ca realm abc pem filename rootca.pem
   ```

   After the CA certificate has been imported successfully, check CA certificate information.

   ```
   [Huawei] display pki certificate ca realm abc
   ```

4. Import the local certificate.

   For example, the obtained local certificate file is named **localcert.pem**.

   ```
   [Huawei] pki import-certificate local realm abc pem filename localcert.pem
   ```

   After the local certificate has been imported successfully, check local certificate information.

   ```
   [Huawei] display pki certificate local realm abc
   ```

5. Import the RSA key pair. For the files in PEM or PKCS#12 format, the password for the RSA key pair provided by the CA is also required.

   For example, the obtained RSA key pair file is **local_privatekey.pem**, and the password is **Huawei@123**.

   ```
   [Huawei] pki import rsa-key-pair abc pem local_privatekey.pem password Huawei@123
   ```

   After the RSA key pair has been imported successfully, check RSA key pair information.

   ```
   [Huawei] display pki rsa local-key-pair name abc public
   ```

6. Check whether the imported local certificate and RSA key pair match. If no matching key pair is found, check whether the imported file is correct.

   ```
   [Huawei] pki match-rsa-key certificate-filename localcert.pem
   Info: The file localcert.pem contains certificates 1.
   Info: Certificate 1 from file localcert.pem matches RSA key test.
   ```

 Copyright © Huawei Technologies Co., Ltd. 

# 17 SSL Configuration

## About This Chapter

17.1 Overview of SSL

17.2 Licensing Requirements and Limitations for SSL

17.3 Default Settings for SSL

17.4 Configuring a Server SSL Policy

17.5 Configuring a Client SSL Policy

17.6 Maintaining SSL

17.7 Configuration Examples for SSL

## 17.1 Overview of SSL

### Overview

The Secure Sockets Layer (SSL) protocol uses data encryption, identity authentication, and message integrity check to ensure security of TCP-based application layer protocols.

SSL is a cryptographic protocol that provides communication security over the Internet. It allows a client and a server to communicate in a way designed to prevent eavesdropping. The server must be authenticated by the client before they start to communicate, and the client can also be authenticated by the server. SSL is widely used in ecommerce and online banking. It has the following advantages:

- High security: SSL ensures secure data transmission by using data encryption, identity authentication, and message integrity check.
- Support for various application layer protocols: SSL was originally designed to secure World Wide Web traffic. SSL functions between the application layer and the transport layer, so it can provide security for any TCP-based application.

 Copyright © Huawei Technologies Co., Ltd. 

- Easy to deploy: SSL has become a world-wide communications standard used to authenticate websites and web users, and to encrypt data transmitted between browser users and web servers.

SSL improves device security using the following functions:

- Allows only authorized users to connect to servers.
- Encrypts data transmitted between a client and a server to secure data transmission and computes a digest to ensure data integrity.
- Defines an access control policy on a device based on certificate attributes to control access rights of clients. This access control policy prevents unauthorized users from attacking the device.

## Basic Concepts

- Certificate Authority (CA)

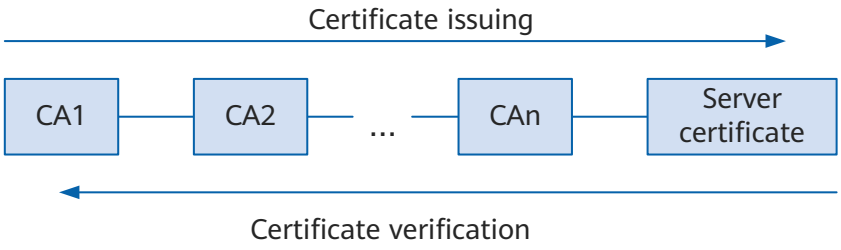
  A CA is an entity that issues, manages, and abolishes digital certificates. A CA checks validity of digital certificate owners, signs digital certificates to prevent eavesdropping and tampering, and manages certificates and keys. A world-wide trusted CA is called a root CA. The root CA can authorize other CAs as subordinate CAs. The CA identities are described in a trusted-CA file.

  In the certificate issuing process, CA1 functions as the root CA and issues a certificate for CA2, and CA2 issues a certificate for CA3. The process repeats until CAn issues the final server certificate.

  In the certificate authentication process, the client first authenticates the server's certificate. If CA3 issues the server certificate, the client uses CA3 certificate to authenticate the server certificate. If the server certificate is authenticated, the client uses CA2 certificate to authenticate the CA3 certificate. After CA2 certificate is authenticated, the client uses CA1 certificate to authenticate CA2 certificate. The client considers the server certificate valid only when CA2 certificate has been authenticated.

  **Figure 17-1** shows the certificate issuing and authentication processes.

  **Figure 17-1** Certificate issuing and authentication

- Digital certificate

  A digital certificate is an electronic document issued by a CA to bind a public key with a certificate subject (an applicant that has obtained a certificate). Information in a digital certificate includes the applicant name, public key, digital signature of the CA that issues the digital certificate, and validity period of the digital certificate. A digital certificate verifies the identities of two communicating parties, improving communication reliability.

  A user must obtain the public key certificate of the information sender to decrypt and authenticate information in the certificate. The user also needs

 Copyright © Huawei Technologies Co., Ltd. 

the CA certificate of the information sender to verify the identity of the information sender.

- Certificate Revocation List (CRL)

  A CRL is issued by a CA to specify certificates that have been revoked.

  Each certificate has a validity period. A CA can issue a CRL to revoke certificates before their validity periods expire. The validity period of a certificate specified in the CRL is shorter than the original validity period of the certificate. If a CA revokes a digital certificate, the key pair defined in the certificate cannot be used. After a certificate in a CRL expires, the certificate is deleted from the CRL to shorten the CRL.

  Information in a CRL includes the issuer and serial number of each certificate, the issuing date of the CRL, certificate revocation date, and time when the next CRL will be issued.

  Clients use CRLs to check validity of certificates. When verifying a server's digital certificate, a client checks the CRL. If the certificate is in the CRL, the client considers the certificate invalid.

## Security Mechanisms

SSL provides the following security mechanisms:

- Connection privacy

  SSL uses symmetric cryptography to encrypt data. It uses the Rivest-Shamir-Adleman (RSA) algorithm (an asymmetric algorithm) to encrypt the key used by the symmetric cryptography.

- Identity authentication

  Digital certificates are used to authenticate a server and a client that need to communicate with each other. The SSL server and client use the mechanism provided by the public key infrastructure (PKI) to apply to a CA for a certificate.

- Message integrity

  A keyed message authentication code (MAC) is used to verify message integrity during transmission.

  A MAC algorithm computes a key and data of an arbitrary length to generate a MAC of a fixed length.

  – A message sender uses a MAC algorithm and a key to compute a MAC, appends it to a message, and send the message to a receiver.
  – The receiver uses the same key and MAC algorithm to compute a MAC and compares it with the MAC in the received message.

  If the two MACs are the same, the message has not been tampered during transmission. If the two MACs are different, the message has been tampered with, and the receiver discards this message.

# 17.2 Licensing Requirements and Limitations for SSL

## Involved Network Elements

- SSL server

 Copyright © Huawei Technologies Co., Ltd. 

- SSL client

### Licensing Requirements

The SSL function is not under license control.

### Feature Limitations

None

## 17.3 Default Settings for SSL

Table 17-1 describes the default settings for SSL.

**Table 17-1** Default settings for SSL

| Parameter | Default Setting |
| --- | --- |
| SSL protocol version in a client SSL policy | TLS1.2 |
| Cipher suite in a client SSL policy | rsa_aes_128_sha256 and rsa_aes_256_sha256 |
| Cipher suite in a server SSL policy | rsa_aes_128_sha256 and rsa_aes_256_sha256 |
| Maximum number of sessions that can be saved and timeout period of a saved session | By default, a maximum of 3600 sessions can be saved, and the timeout period of a saved session is as follows:<br>• AR100&AR120&AR150&AR160&AR200 series: 32<br>• AR1200 series: 128<br>• AR2200 series: 128<br>• AR3200 series: 256<br>• AR3600 series: 256 |

## 17.4 Configuring a Server SSL Policy

### Prerequisites

The **PKI domain** has been configured.

### Context

The SSL protocol uses data encryption, identity authentication, and message integrity check to ensure security of TCP-based application layer protocols. To use an Router as an SSL server, configure a server SSL policy on the Router. A server

 Copyright © Huawei Technologies Co., Ltd. 

SSL policy can be applied to application layer protocols such as HTTP to provide secure connections.

**Figure 17-2** Router functions as an SSL server




As shown in **Figure 17-2**, the Router functions as an SSL server and has a server SSL policy configured. During an SSL handshake, the Router uses the SSL parameters in the server SSL policy to negotiate session parameters with an SSL client. After the handshake is complete, the Router establishes a session with the client.

When functioning as an SSL server, the Router is authenticated by the SSL client, but it cannot authenticate the client.

NOTE

When functioning as an SSL server, the Router can communicate with SSL clients running SSL3.0, TLS1.0, TLS1.1 and TLS1.2.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **ssl policy** *policy-name* **type server**

A server SSL policy is created, and the server SSL policy view is displayed.

**Step 3** Run **pki-realm** *realm-name*

A PKI domain is specified for the server SSL policy.

By default, no PKI domain is specified for a server SSL policy on the Router.

NOTE

The Router obtains a digital certificate from a CA in the specified PKI domain. SSL clients can then authenticate the Router by checking the digital certificate.

The Router can also generate self-signed certificates. However, the device does not provide life cycle management for self-signed certificates. For example, self-signed certificates cannot be updated, or revoked on the device. To ensure security of the device and certificates, it is recommended the user's certificate be used.

**Step 4** (Optional) Run **version** { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** } *

The SSL protocol version is specified.

By default, a server SSL policy uses Transport Layer Security (TLS) version 1.2.

NOTE

TLS1.2 version is recommended, other protocol version has potential security risks.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 5** (Optional) Run **session** { **cachesize** *size* | **timeout** *time* } *

The maximum number of sessions that can be saved and the timeout period of a saved session are set.

By default, a maximum of 3600 sessions can be saved, and the timeout period of a saved session is as follows:

- AR100&AR120&AR150&AR160&AR200 series: 32
- AR1200 series: 128
- AR2200 series: 128
- AR3200 series: 256
- AR3600 series: 256

**Step 6** (Optional) Run **ciphersuite** { **rsa_3des_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_sha256** | **rsa_aes_256_sha256** | **rsa_aes128_ccm** | **rsa_aes128_gcm_sha256** | **rsa_aes256_ccm** | **rsa_aes256_gcm_sha384** | **ecdhe_rsa_aes128_gcm_sha256** | **ecdhe_rsa_aes256_gcm_sha384** } *

A cipher suite is specified.

By default, a server SSL policy supports the cipher suites: **ecdhe_rsa_aes128_gcm_sha256**, **ecdhe_rsa_aes256_gcm_sha384**, **rsa_aes_128_sha256**, and **rsa_aes_256_sha256**.

**Step 7** (Optional) Configure the SSL renegotiation function.

Disabling the renegotiation function on the device can protect the device against renegotiation attacks, but will interrupt services. Therefore, you can keep the renegotiation function enabled, and set the SSL renegotiation rate to minimize the impact of renegotiation attacks on services. Choose either of the following tasks:

- Disable renegotiation.

  Run the **undo renegotiation enable** command to disable SSL renegotiation.

  By default, SSL renegotiation is enabled.
- Set the renegotiation rate.
  a. Run the **quit** command to return to the system view.
  b. Run the **ssl renegotiation-rate** *rate* command to set the SSL renegotiation rate.

     By default, the SSL renegotiation is performed once per second. You can set the rate according to the CPU capability of the device.

     This configuration applies to all SSL policies.

**----End**

## Verifying the Configuration

Run the **display ssl policy** [ *policy-name* ] command to view the configuration of the SSL policy.

# 17.5 Configuring a Client SSL Policy

 Copyright © Huawei Technologies Co., Ltd. 

## Prerequisites

The **PKI domain** has been configured.

## Context

The SSL protocol uses data encryption, identity authentication, and message integrity check to ensure security of TCP-based application layer protocols. A client SSL policy can be applied to application layer protocols such as the CPE WAN Management Protocol (CWMP) to provide secure connections.

**Figure 17-3** Router functions as an SSL client




As shown in **Figure 17-3**, the **Figure 17-3** functions as an SSL client and has a client SSL policy configured. During an SSL handshake, the Router uses the SSL parameters in the client SSL policy to negotiate session parameters with the SSL server. After the handshake is complete, the Router establishes a session with the server.

When functioning as an SSL client, the Router does not allow SSL servers to authenticate it, but it can authenticate SSL servers. When the Router functions as an SSL client, enable it to authenticate servers to ensure secure communication.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **ssl policy** *policy-name* **type client**

A client SSL policy is created, and the client SSL policy view is displayed.

**Step 3** Run **server-verify enable**

SSL server authentication is enabled.

By default, SSL server authentication is enabled in a client SSL policy.

**Step 4** Run **pki-realm** *realm-name*

A PKI domain is specified for the client SSL policy.

By default, no PKI domain is specified for a client SSL policy on the Router.

NOTE

The Router obtains a CA certificate chain from CAs in the specified PKI domain. The Router authenticates an SSL server by checking the server certificate and CA certificates against the CA certificate chain.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 5** (Optional) Run **version** { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** }

The SSL protocol version is specified.

By default, a client SSL policy uses Transport Layer Security (TLS) version 1.2.

NOTE

Ensure that the specified SSL protocol version is supported by the SSL server. Before performing this step, check the SSL protocol versions that the SSL server supports.

TLS1.2 version is recommended, other protocol version has potential security risks.

**Step 6** (Optional) Run **prefer-ciphersuite** { **rsa_3des_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_sha256** | **rsa_aes_256_sha256** | **rsa_aes128_ccm** | **rsa_aes128_gcm_sha256** | **rsa_aes256_ccm** | **rsa_aes256_gcm_sha384** | **ecdhe_rsa_aes128_gcm_sha256** | **ecdhe_rsa_aes256_gcm_sha384** } *

A cipher suite is specified.

By default, a client SSL policy uses the cipher suites: **ecdhe_rsa_aes128_gcm_sha256**, **ecdhe_rsa_aes256_gcm_sha384**, **rsa_aes_128_sha256**, and **rsa_aes_256_sha256**.

NOTE

Ensure that the specified cipher suite is supported by the SSL server. Before performing this step, check the cipher suites that the SSL server supports.

**Step 7** (Optional) Configure the SSL renegotiation function.

Disabling the renegotiation function on the device can protect the device against renegotiation attacks, but will interrupt services. Therefore, you can keep the renegotiation function enabled, and set the SSL renegotiation rate to minimize the impact of renegotiation attacks on services. Choose either of the following tasks:

- Disable renegotiation.

  Run the **undo renegotiation enable** command to disable SSL renegotiation.

  By default, SSL renegotiation is enabled.
- Set the renegotiation rate.
  a. Run the **quit** command to return to the system view.
  b. Run the **ssl renegotiation-rate** *rate* command to set the SSL renegotiation rate.

     By default, the SSL renegotiation is performed once per second. You can set the rate according to the CPU capability of the device.

     This configuration applies to all SSL policies.

**----End**

## Verifying the Configuration

Run the **display ssl policy** [ *policy-name* ] command to view the configuration of the SSL policy.

 Copyright © Huawei Technologies Co., Ltd. 

# 17.6 Maintaining SSL

## 17.6.1 Viewing Statistics on SSL Connections

### Context

When a device sets up a connection with an SSL server or client, the device automatically counts and records the SSL connection.

Statistics on SSL connections help the administrator perform SSL fault diagnosis and troubleshooting.

### Procedure

- Run the **display ssl connection statistics** command to view SSL connection statistics.

**----End**

## 17.6.2 Deleting Statistics on SSL Connections

### Context

Before counting the maximum number of SSL connections within a certain period of time, delete the existing SSL statistics first.

NOTE

SSL statistics cannot be restored after you delete them. So, confirm the action before you use the command.

### Procedure

- Run the **reset ssl connection statistics** command to delete SSL statistics.

**----End**

# 17.7 Configuration Examples for SSL

## 17.7.1 Example for Configuring a Server SSL Policy

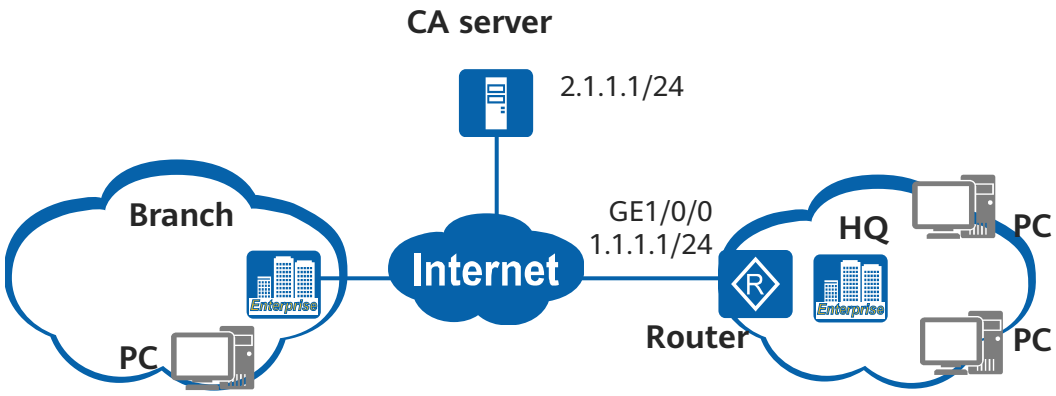
### Networking Requirements

As shown in **Figure 17-4**, enterprise users use a web browser to connect to the Router. To prevent eavesdropping and tampering during data transmission, a network administrator requires users to use HTTPS to access the Router securely.

 Copyright © Huawei Technologies Co., Ltd. 

To meet this requirement, configure the Router as an HTTPS server and associate the HTTPS server with a server SSL policy so that users can securely access and manage the device through web pages.

**Figure 17-4** Networking diagram of the server SSL policy configuration




## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a PKI entity and a PKI domain.
2. Configure a server SSL policy.
3. Configure the Router as an HTTPS server.

## Procedure

**Step 1** Configure a PKI entity and a PKI domain.

# Configure a PKI entity.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] pki entity users
[Router-pki-entity-users] common-name hello
[Router-pki-entity-users] country cn
[Router-pki-entity-users] state jiangsu
[Router-pki-entity-users] organization huawei
[Router-pki-entity-users] organization-unit info
[Router-pki-entity-users] quit
```

NOTE

If the entity name and entity common name are not set to the Router's IP address 1.1.1.1, the system will display a message indicating that the certificate is invalid when the client opens a website. This does not affect HTTPS application.

# Configure a PKI domain, and enable the automatic certificate enrollment and update function.

```
[Router] pki realm users
[Router-pki-realm-users] entity users
[Router-pki-realm-users] ca id ca_root
[Router-pki-realm-users] enrollment-url http://2.1.1.1:8080/certsrv/mscep/mscep.dll ra
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router-pki-realm-users] fingerprint sha2
7bb05ada0482273388ed4ec228d79f77309ea3f47bb05ada0482273388ed4ec2
[Router-pki-realm-users] auto-enroll regenerate
[Router-pki-realm-users] quit
```

**Step 2** Configure a server SSL policy **sslserver**.

# Create a server SSL policy and specify PKI domain **users** in the policy. This allows the Router to obtain a digital certificate from the CA specified in the PKI domain.

```
[Router] ssl policy sslserver type server
[Router-ssl-policy-sslserver] pki-realm users
```

# Set the maximum number of sessions that can be saved and the timeout period of a session.

```
[Router-ssl-policy-sslserver] session cachesize 40 timeout 7200
[Router-ssl-policy-sslserver] quit
```

**Step 3** Configure the Router as an HTTPS server.

# Apply the SSL policy **sslserver** to the HTTPS service.

```
[Router] http secure-server ssl-policy sslserver
```

# Enable the HTTPS server function on the Router.

```
[Router] http secure-server enable
```

# Configure the port number of the HTTPS service.

```
[Router] http secure-server port 1278
```

**Step 4** Verify the configuration.

# Run the **display ssl policy sslserver** command to view the configuration of the SSL policy **sslserver**.

```
[Router] display ssl policy sslserver
 ------------------------------------------------------------------------------
 Policy name                       :  sslserver
 Policy ID                         :  1
 Policy type                       :  Server
 Cipher suite                      :  rsa_aes_128_cbc_sha
 PKI realm                         :  users
 Version                           :  tls1.1
 Cache number                      :  40
 Time out(second)                  :  7200
 Server certificate load status    :  loaded
 CA certificate chain load status  :  loaded
 SSL renegotiation status          :  enable
 Bind number                       :  1
 SSL connection number             :  0
 ------------------------------------------------------------------------------
```

# Start the web browser on a PC, and enter **https://1.1.1.1:1278** in the address box. The web management system of the Router is displayed, and you can manage the Router on the web pages.

**----End**

## Configuration Files

Router configuration file

 Copyright © Huawei Technologies Co., Ltd. 

```
#
 sysname Router
#
pki entity users
 country CN
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
#
pki realm users
 ca id ca_root
 enrollment-url http://2.1.1.1:8080/certsrv/mscep/mscep.dll ra
 entity users
 auto-enroll regenerate
 fingerprint sha2 7bb05ada0482273388ed4ec228d79f77309ea3f47bb05ada0482273388ed4ec2
#
ssl policy sslserver type server
 pki-realm users
 session cachesize 40 timeout 7200
#
 http secure-server port 1278
 http secure-server ssl-policy sslserver
 http secure-server enable
#
return
```

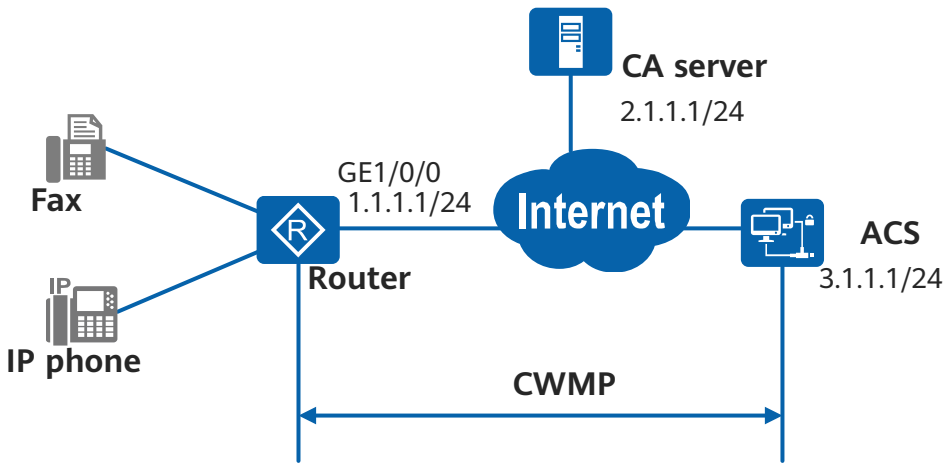
## 17.7.2 Example for Configuring a Client SSL Policy

### Networking Requirements

As shown in **Figure 17-5**, the Router functions as a CPE to connect to phones, and fax machines. An ACS uses CWMP to manage and control the Router.

The ACS functions as an SSL server and has obtained a digital certificate from the CA. You need to configure the Router as an SSL client to authenticate the ACS. This ensures privacy and integrity of data exchanged between the Router and the ACS.

**Figure 17-5** Networking diagram of the client SSL policy configuration




 Copyright © Huawei Technologies Co., Ltd. 

## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a PKI entity and a PKI domain.
2. Configure a client SSL policy on the Router and enable SSL server authentication in the policy.
3. Apply the client SSL policy to the CWMP service so that the Router authenticates the ACS to ensure data privacy and integrity.
4. Enable the Router to automatically initiate connections to the ACS and set the CWMP parameters. This enables the ACS to manage and control the Router using CWMP.

## Procedure

**Step 1** Configure an IP address for the GE1/0/0 interface

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 1.1.1.1 24
[Router-GigabitEthernet1/0/0] quit
```

**Step 2** Configure a PKI entity and a PKI domain.

# Configure a PKI entity.

```
[Router] pki entity cwmp0
[Router-pki-entity-cwmp0] common-name hello
[Router-pki-entity-cwmp0] country cn
[Router-pki-entity-cwmp0] state jiangsu
[Router-pki-entity-cwmp0] organization huawei
[Router-pki-entity-cwmp0] organization-unit info
[Router-pki-entity-cwmp0] quit
```

# Configure a PKI domain, and enable the automatic certificate enrollment and update function.

```
[Router] pki realm cwmp0
[Router-pki-realm-cwmp0] entity cwmp0
[Router-pki-realm-cwmp0] ca id ca_root
[Router-pki-realm-cwmp0] enrollment-url http://2.1.1.1:8080/certsrv/mscep/mscep.dll ra
[Router-pki-realm-cwmp0] fingerprint sha2
7bb05ada0482273388ed4ec228d79f77309ea3f47bb05ada0482273388ed4ec2
[Router-pki-realm-cwmp0] auto-enroll regenerate
[Router-pki-realm-cwmp0] quit
```

**Step 3** Configure a client SSL policy.

# Enable SSL server authentication.

```
[Router] ssl policy sslclient type client
[Router-ssl-policy-sslclient] server-verify enable
```

# Specify the PKI domain **cwmp0** in the client SSL policy.

```
[Router-ssl-policy-sslclient] pki-realm cwmp0
[Router-ssl-policy-sslclient] quit
```

**Step 4** Enable the CWMP function on the Router.

 Copyright © Huawei Technologies Co., Ltd. 

```
[Router] cwmp
[Router-cwmp] cwmp enable
```

**Step 5** Apply the SSL policy to CWMP.

```
[Router-cwmp] cwmp ssl-client ssl-policy sslclient
```

**Step 6** Configure the Router to automatically initiate connections to the ACS.

# Configure the URL used by the Router to connect to the ACS.

```
[Router-cwmp] cwmp acs url https://www.acs.com:80/acs
```

# Enable the Router to send Inform messages.

```
[Router-cwmp] cwmp cpe inform interval enable
```

# Set the interval at which the Router sends Inform messages to 1000 seconds.

```
[Router-cwmp] cwmp cpe inform interval 1000
```

# Configure the Router to send an Inform message at 2011-01-01 20:00:00.

```
[Router-cwmp] cwmp cpe inform time 2011-01-01T20:00:00
```

**Step 7** Set CWMP parameters on the Router.

# Configure the interface that the Router uses to connect to the ACS.

```
[Router-cwmp] cwmp cpe connect interface gigabitethernet 1/0/0
```

# Set the user name and password that the Router uses for authentication by the ACS.

```
[Router-cwmp] cwmp acs username newacsname
[Router-cwmp] cwmp acs password cipher newacspsw
```

# Configure the user name and password that the Router uses to authenticate the ACS.

```
[Router-cwmp] cwmp cpe username newcpename
[Router-cwmp] cwmp cpe password cipher newcpepsw
```

# Set the maximum number of connection attempts to 5.

```
[Router-cwmp] cwmp cpe connect retry 5
```

# Set the close-wait timer of the Router to 100 seconds. If no data is transmitted within 100 seconds, the connection is torn down.

```
[Router-cwmp] cwmp cpe wait timeout 100
```

**Step 8** Verify the configuration.

# Run the **display current-configuration** command. The command output shows that SSL has been successfully configured for CWMP.

```
<Router> display current-configuration
...
cwmp
 cwmp cpe inform interval enable
 cwmp acs url https://www.acs.com:80/acs
 cwmp acs username newacsname
 cwmp acs password cipher %@%@"\~.1[)4MGN=d\4zy`$,"ne\%@%@
 cwmp cpe username newcpename
 cwmp cpe password cipher %@%@"\~.1[)4MGN=d\4zy`$,"ne\%@%@
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 cwmp cpe inform interval 1000
 cwmp cpe connect retry 5
 cwmp cpe wait timeout 100
 cwmp cpe connect interface GigabitEthernet 1/0/0
 cwmp ssl-client ssl-policy sslclient
...
```

# Run the **display cwmp configuration** command. The command output shows that CWMP is enabled, and the Router is configured to send Inform packets at intervals.

```
<Router> display cwmp configuration
  CWMP is enabled
  ACS URL:                      https://www.acs.com:80/acs
  ACS username:                   newacsname
  ACS password:                   %@%@"\~.1[)4MGN=d\4zy`$,"ne\%@%@
  Inform enable status:           enabled
  Inform interval:              1000s
  Inform time:                  2011-01-01T20:00:00
  Wait timeout:                 100s
  Reconnection times:             5
```

# Run the **display cwmp status** command. The command output shows that CWMP is enabled, and the CWMP connection status is **connected**.

```
<Router> display cwmp status
 CWMP is enabled
 ACS URL:                      https://www.acs.com:80/acs
 Acs information is set by:          user
 ACS username:                 newacsname
 ACS password:                 %@%@.h(P;/FO7%q"9H6D1]/O"90'%@%@
 Connection status:            connected
 Time of last successful connection:   2010-12-01T20:00:00
```

**----End**

## Configuration Files

Router configuration file

```
#
 sysname Router
#
interface GigabitEthernet 1/0/0
 ip address 1.1.1.1 255.255.255.0
#
cwmp
 cwmp cpe inform interval enable
 cwmp acs url https://www.acs.com:80/acs
 cwmp acs username newacsname
 cwmp acs password cipher %@%@"\~.1[)4MGN=d\4zy`$,"ne\%@%@
 cwmp cpe username newcpename
 cwmp cpe password cipher %@%@"\~.1[)4MGN=d\4zy`$,"ne\%@%@
 cwmp cpe inform interval 1000
 cwmp cpe connect retry 5
 cwmp cpe wait timeout 100
 cwmp cpe connect interface GigabitEthernet 1/0/0
 cwmp ssl-client ssl-policy sslclient
#
pki entity cwmp0
 country CN
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
```

 Copyright © Huawei Technologies Co., Ltd. 

```
#
pki realm cwmp0
 ca id ca_root
 enrollment-url http://2.1.1.1:8080/certsrv/mscep/mscep.dll ra
 entity cwmp0
 auto-enroll regenerate
 fingerprint sha2 7bb05ada0482273388ed4ec228d79f77309ea3f47bb05ada0482273388ed4ec2
#
ssl policy sslclient type client
 server-verify enable
 pki-realm cwmp0
#
return
```

# 18 HTTPS Configuration

## About This Chapter

The Hypertext Transfer Protocol Secure (HTTPS) protocol provides secure web access using security mechanisms provided by the Secure Sockets Layer (SSL) protocol, including data encryption, identity authentication, and message integrity check.

18.1 Overview of HTTPS
18.2 Licensing Requirements and Limitations for HTTPS
18.3 Configuring the Device as an HTTPS Server
18.4 Configuration Examples for HTTPS

## 18.1 Overview of HTTPS

Secure HTTP (HTTPS) supports the secure sockets Layer (SSL).

HTTPS improves device security using SSL:

- Allows authorized clients access the device securely and rejects unauthorized clients
- Encrypts data exchanged between clients and the device to ensure data transmission security and integrity and implement secure management.
- Defines access control policies based on certificate attributes and controls access rights of clients to defend against attacks from unauthorized clients.

As shown in **Figure 18-1**, an SSL policy is configured on the device (an HTTP server). After the HTTPS server function is enabled on the device, users can use a web browser to log in to the device (an HTTPS server) and manage the device on web pages.

**Figure 18-1** Logging in to an HTTPS server through the web browser




 Copyright © Huawei Technologies Co., Ltd. 

# 18.2 Licensing Requirements and Limitations for HTTPS

## Involved Network Elements

Other network elements are not required.

## Licensing Requirements

HTTPS is a basic feature of the router and is not under license control.

## Feature Limitations

None

# 18.3 Configuring the Device as an HTTPS Server

## Prerequisites

A server SSL policy has been configured. For details on how to configure a server SSL policy, see **Configuring a Server SSL Policy**.

## Context

The HTTPS server function allows users to securely access the device on web pages.

When users access a remote device functioning as an HTTP server, the following problems exist:

- Users cannot authenticate the device.
- Privacy and integrity of data transmitted between users and the device cannot be ensured.

To solve the preceding problems, configure the device as an HTTPS server. The device uses the SSL protocol's data encryption, identity authentication, and message integrity check mechanisms to protect security of data transmitted between users and the device. These mechanisms ensure that users securely access a remote device on web pages.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **http secure-server ssl-policy** *ssl-policy*

An SSL policy is applied to the HTTPS service.

By default, the server SSL policy applied to the HTTPS service on the device is default_policy.

 Copyright © Huawei Technologies Co., Ltd. 

**Step 3** (Optional) Run **http secure-server port** *port-number*

The port number is set for the HTTPS service.

By default, the port number of the HTTPS service is 443.

**Step 4** (Optional) Run **http secure-server manager-port** *port-number*

The management port of the HTTPS server is enabled and the management port number is set.

By default, the management port of the HTTPS server is disabled.

NOTE

Only users at level 3 and higher levels can log in to the web platform through the management port.

**Step 5** Run **http secure-server enable**

The HTTPS server function is enabled on the device.

By default, the HTTPS server function is enabled on the device.

**----End**

### Verifying the Configuration

# Run the **display current-configuration** command to check the configuration of the HTTPS server.

```
<Huawei> display current-configuration | include http secure-server
 http secure-server port 1026
 http secure-server ssl-policy user
 http secure-server enable
```

# 18.4 Configuration Examples for HTTPS

## 18.4.1 Example for Configuring the Device as an HTTPS Server

### Networking Requirements

As shown in **Figure 18-2**, users access the gateway Router through web.

To prevent data intercepting and tampering during data transmission, a network administrator requires that users use HTTPS to access the Router securely.

**Figure 18-2** Networking diagram of HTTPS server configuration




 Copyright © Huawei Technologies Co., Ltd. 

## Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN and a VLANIF interface, and configure the interface to allow enterprise users to access the router.
2. Configure a server SSL policy and apply the default PKI domain to the server SSL policy. The CA server is not required.
3. Configure an HTTPS server to ensure confidentiality and integrity of data transmission between users and the Router.

## Procedure

**Step 1** Create a VLAN and configure the interface.

# Create VLAN 11 on the Router.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 11
```

# Add Eth2/0/0 connecting to users to VLAN 11.

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type access
[Router-Ethernet2/0/0] port default vlan 11
[Router-Ethernet2/0/0] quit
```

# Create VLANIF 11 and assign IP address 10.1.1.1/24 to VLANIF 11.

```
[Router] interface vlanif11
[Router-Vlanif11] ip address 10.1.1.1 24
[Router-Vlanif11] quit
```

**Step 2** Configure a server SSL policy.

# Apply the default PKI domain **default** to the server SSL policy.

```
[Router] ssl policy userserver type server
[Router-ssl-policy-userserver] pki-realm default
```

# Set the maximum number of sessions that can be saved and the timeout period of a saved session are set.

```
[Router-ssl-policy-userserver] session cachesize 20 timeout 7200
[Router-ssl-policy-userserver] quit
```

**Step 3** Configure the HTTPS server.

# Bind the SSL policy **userserver** to the HTTPS server.

```
[Router] http secure-server ssl-policy userserver
```

# Configure the port number of the HTTPS service.

```
[Router] http secure-server port 1278
```

# Enable the HTTPS server function on the Router.

```
[Router] http secure-server enable
Warning: The HTTP server has not configured with SSL policy. Continue starting HTTP secure server? [Y/N]:
y
  This operation will take several minutes, please wait.....................................................
Info: Succeeded in starting the HTTPS server
```

 Copyright © Huawei Technologies Co., Ltd. 

**Step 4** Verify the configuration.

# Run the **display ssl policy userserver** command to view the configuration of the SSL policy **userserver**.

```
[Router] display ssl policy userserver
  ------------------------------------------------------------------------------
  Policy name                        :  userserver
  Policy ID                          :  2
  Policy type                        :  Server
  Cipher suite                       :  rsa_aes_128_cbc_sha
  PKI realm                          :  default
  Cache number                       :  20
  Time out(second)                   :  7200
  Server certificate load status     :  loaded
  CA certificate chain load status   :  unloaded
  SSL renegotiation status           :  enable
  Bind number                        :  1
  SSL connection number              :  0
  ------------------------------------------------------------------------------
```

# Start the web browser on a computer, and enter https://10.1.1.1:1278 in the address box. The web management system is displayed, and you can manage the Router on the web pages.

**----End**

## Configuration Files

Configuration file of the Router

```
#
 sysname Router
#
ssl policy userserver type server
 pki-realm default
 session cachesize 20 timeout 7200
#
 http secure-server ssl-policy userserver
 http secure-server enable
 http secure-server port 1278
#
vlan batch 11
#
interface Vlanif11
 ip address 10.1.1.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 11
#
return
```

 Copyright © Huawei Technologies Co., Ltd. 

# 19 Keychain Configuration

## About This Chapter

This chapter describes how to configure a keychain to control authentication algorithms and key-string in a centralized way.

19.1 Overview of Keychains

19.2 Understanding Keychains

19.3 Application Scenarios for Keychains

19.4 Licensing Requirements and Limitations for Keychains

19.5 Configuring a Keychain

19.6 Configuration Examples for Keychains

## 19.1 Overview of Keychains

### Definition

A keychain is a set of encryption rules, called keys. It authenticates applications and dynamically changes algorithms and keys during authentication. The keychain periodically changes authentication keys and algorithms to improve transmission, without interrupting services.

### Purpose

When two applications communicate, some unauthorized users may try to modify data packets or forge authorized users on the network, which may cause security problems. To identify modified packets and forged users, applications authenticate information by defining authentication rules. An application may use independent authentication rules.

However, an authentication rule may be cracked by unauthorized users if it is used for a long time. Modifying authentication rules by administrators is complicated

 Copyright © Huawei Technologies Co., Ltd. 

and may cause faults. Besides, if each application has an independent authentication rule, many applications may use the same authentication mode, duplicating data and configuration.

Therefore, the keychain is used to manage all the authentication algorithms and keys. The keychain can control the authentication and dynamically change algorithms and key strings during authentication, which improves communication security.

# 19.2 Understanding Keychains

## 19.2.1 Basic Concepts of Keychains

A keychain is a set of encryption rules, called keys. A key includes an algorithm, a key string, and the send/receive time. The algorithm and key string are used to encrypt and decrypt packets. The send and receive time indicate that during the period, packets are sent and received using the algorithm and key string.

### key

A key includes an algorithm, a key string, and the send/receive time. The keychain support algorithms such as MD5, SHA-1, SHA-256, HMAC-MD5, HMAC-SHA1-12, and HMAC-SHA1-20. An application must support the algorithm configured in the keychain if the keychain is applied to the application. The key string is a string configured by users.

The active time includes the active send time and the active receive time. The device dynamically changes keys by setting the send and receive time. Keys are classified into the following types:

- Active send key: When the system time is within the send time range, the key is the active send key. When the application sends a packet, the algorithm and key configured by the key generate a Message Authentication Code (MAC) on the sending end.
- Active receive key: When the system time is within the receive time range, the key is the active receive key. When the application receives a packet, the algorithm and key configured by the key generate a MAC on the receiving end.

### Message Authentication Code

A MAC is a character string. The MAC is calculated from data packets and key string using the algorithm.

### Keychain Time Mode

Keychain time has an absolute time mode and a periodic time mode.

Absolute time mode uses the Coordinated Universal Time (UTC) format.

Periodic time mode sets a specific time period during which a keychain functions. Periodic time mode includes the following types:

 Copyright © Huawei Technologies Co., Ltd. 

- **Daily**: The key in a keychain takes effect at a specified time each day.
- **Weekly**: The key in a keychain takes effect on a specified day or days each week.
- **Monthly**: The key in a keychain takes effect on a specified day or days each month.
- **Yearly**: The key in a keychain takes effect in a specified month or months each year.

Only one time mode can be specified in a keychain. The time mode must be specified when the keychain is created. The send time and receive time of the key are configured based on the time mode of the keychain.

## Default Send Key

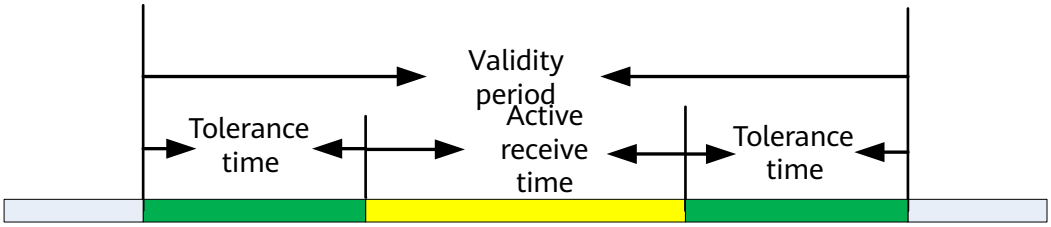
If no key is configured in a period, no send key is active in that period. Therefore, applications do not send authentication packets to each other. A default send key can be configured to prevent this situation. When no other send keys are active, the default send key takes effect.

## Receive Tolerance Time

When the send key on the device changes, the receive key on the receiving end must be changed. A delay may occur when keys change due to time asynchronization. Packets may be lost during this period. To prevent this situation, a smooth transit is needed in the receive key change. The smooth transit time is called the receive tolerance time.

The receive tolerance time only takes effect on the receive key and can be configured on each keychain. As shown in **Figure 19-1**, when the receive tolerance time is configured, the start receive time is advanced and the end receive time is delayed.

**Figure 19-1** Valid Time Range of Tolerance Time




## TCP kind-value and TCP algorithm-id

TCP applications are connected using TCP authentication. TCP uses enhanced TCP authentication options to send TCP authentication packets.

- Vendors use different kind-values to represent the enhanced TCP authentication option. To enable devices of different vendors to communicate with each other, the kind-value can be configured based on the TCP kind of the peer device.
- There is an algorithm-id field in the enhanced TCP authentication option, indicating the type of the algorithm. The algorithm-id is not defined by the Internet Assigned Numbers Authority (IANA), so different vendors use

 Copyright © Huawei Technologies Co., Ltd. 

different algorithm-id to represent algorithms. The mapping between the algorithm-id and the algorithm can be configured to enable devices of different vendors to communicate with each other.

## 19.2.2 Implementation of Keychains for a Non-TCP Application

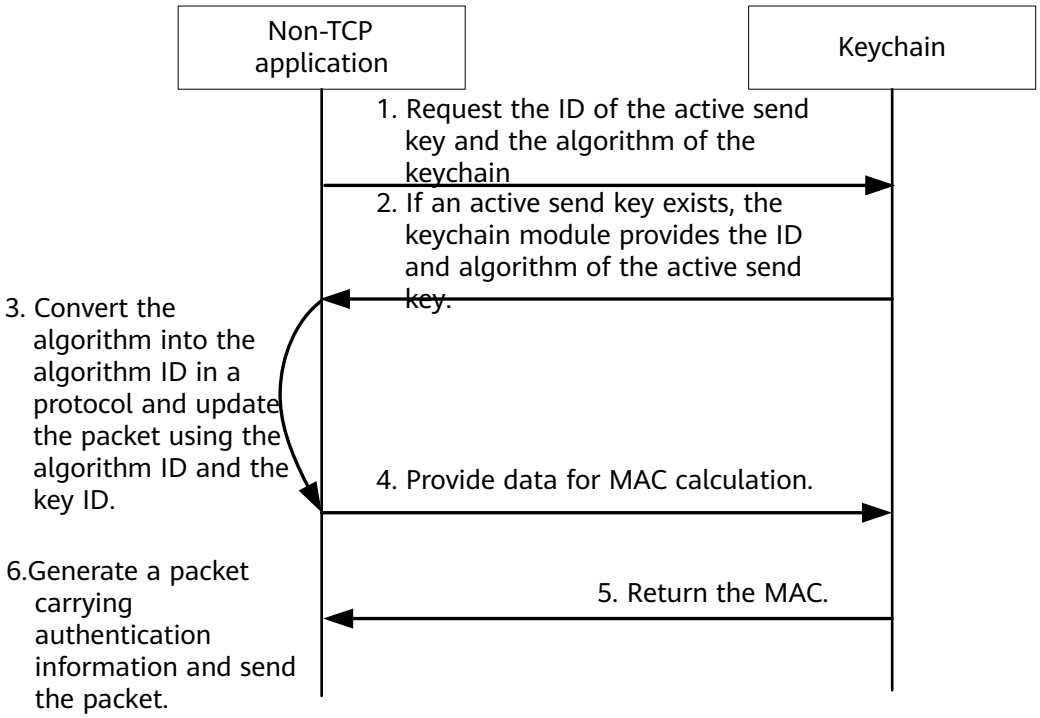
The keychain provides authentication for application-layer protocols. A keychain only takes effect after it is applied to applications. Based on processing procedures, the keychain can be applied to non-TCP applications and TCP applications.

### A Non-TCP Application Sends Packets Using the Keychain

A non-TCP application sends packets using the keychain in the procedures as shown in **Figure 19-2**.

1. The application requests the ID of the active send key and the algorithm of the keychain.
2. If an active send key exists, the keychain module provides the ID and algorithm of the active send key. If no active send key exists, the application sends the packet without encryption.
3. After receiving the ID and algorithm of the active send key, the application converts the algorithm into the algorithm ID in a protocol and encapsulates the algorithm ID and the key ID in the packet.
4. The application provides data for MAC calculation.
5. The keychain module calculates the MAC using the algorithm and key defined by the active send key and returns the MAC to the application.
6. The application generates a packet carrying authentication information and sends the packet.

**Figure 19-2** A non-TCP application sends packets using the keychain



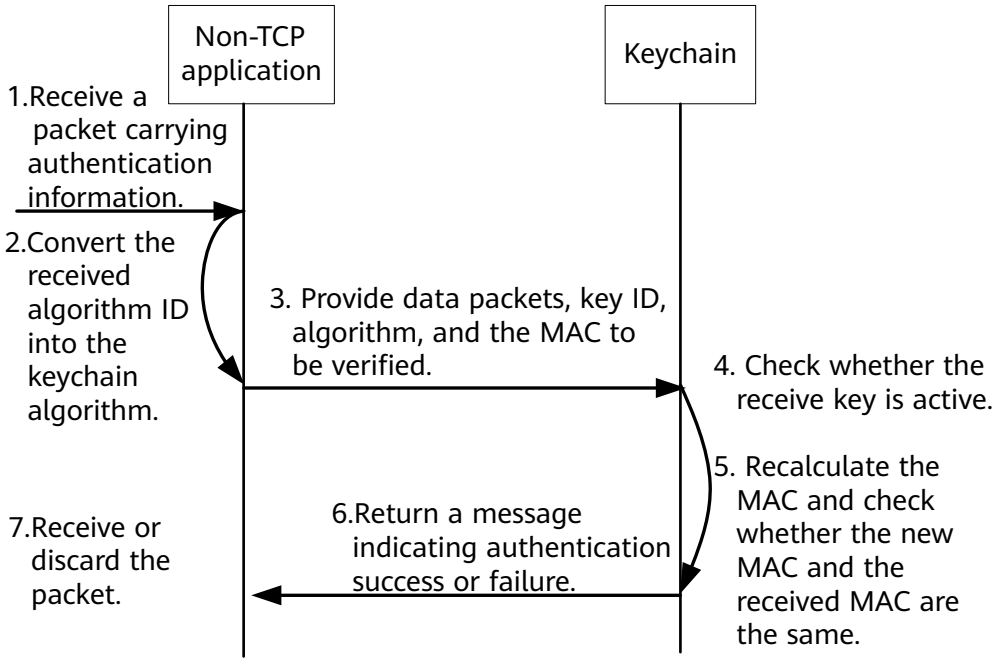

 Copyright © Huawei Technologies Co., Ltd. 

## A Non-TCP Application Receives Packets Using the Keychain

A non-TCP application receives packets using the keychain in the procedures as shown in **Figure 19-3**.

1. The receiving end receives a packet carrying authentication information.
2. The application on the receiving end converts the received algorithm ID into the keychain algorithm.
3. The application on the receiving end provides data packets, key ID, algorithm, and the MAC to be verified.
4. The keychain module checks whether the receive key having the same key ID with the received packet is active. If the receive key is not active, the keychain sends a Reject packet.
5. If the receive key is active, the keychain module uses the algorithm and key string configured on the key to recalculate the MAC and checks whether the new MAC and the received MAC are the same.
6. A message indicating authentication success or failure is returned.
7. The application receives or discards the packets based on the authentication result.

**Figure 19-3** A non-TCP application receives packets using the keychain




**NOTE**

IS-IS uses the keychain authentication and the packet does not carry the key ID. When the receive end receives the IS-IS packet carrying authentication information, the device will check all the active receive keys to find a receive key which has the same algorithm for verification.

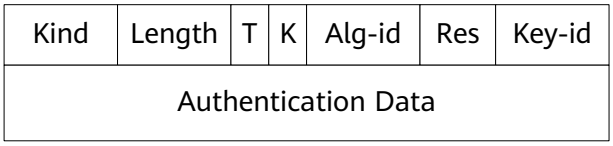
 Copyright © Huawei Technologies Co., Ltd. 

# 19.2.3 Implementation of Keychains for TCP Applications

## TCP Applications Send Packets Using the Keychain

In the donica draft, TCP uses enhanced TCP authentication options to send TCP authentication packets. **Figure 19-4** shows the format of the enhanced authentication option packet:

**Figure 19-4** Format of enhanced TCP authentication option



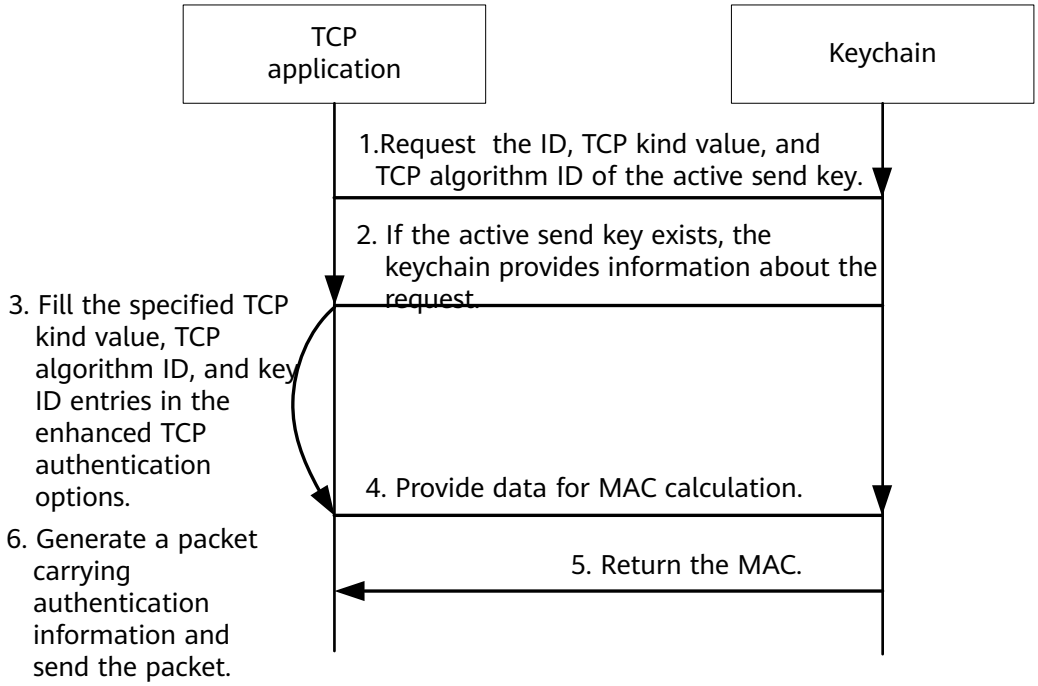

The Bonica draft has not been standardized, and IANA has not defined the kind value and algorithm ID. Vendors use different kind values and algorithm IDs. To enable devices of different vendors to communication with each other, you can configure the TCP kind value and the mapping between the TCP algorithm and algorithm ID.

The command output is as follows: A TCP application sends packets using the keychain in the procedures as shown in **Figure 19-5**.

1. The application requests the ID, TCP kind value, and TCP algorithm ID of the active send key.
2. If the active send key exists, the keychain provides information about the request.
3. The application fills the specified TCP kind value, TCP algorithm ID, and key ID entries in the enhanced TCP authentication options.
4. The application provides data for MAC calculation.
5. The keychain module calculates the MAC based on the algorithm and key string configured for the active send key and returns the MAC.
6. The application fills the MAC entry in the enhanced TCP authentication options and sends the packet.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 19-5** A TCP application sends packets using the keychain



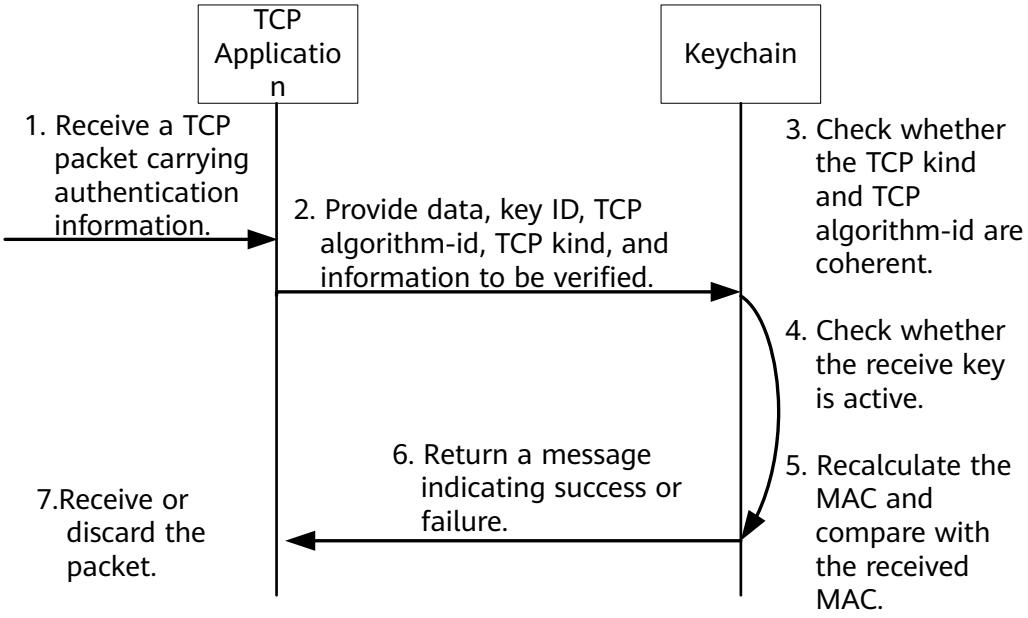

## A TCP Application Receives Packets Using the Keychain

A TCP application receives packets using the keychain in the procedures, as shown in **Figure 19-6**.

1. The receiving end receives a TCP packet carrying authentication information.
2. The receiving end provides data packets, key ID, TCP algorithm ID, TCP kind value, and the MAC to be verified for the keychain.
3. The keychain checks whether the TCP type value and algorithm ID in the received packet is the same as those in the local end. If not, the keychain sends a Reject packet.
4. The keychain module checks whether the receive key having the same key ID with the received packet is active. If the receive key is not active, the keychain sends a Reject packet.
5. If the receive key is active, the keychain module uses the algorithm and key string configured on the key to recalculate the MAC and checks whether the new MAC and the received MAC are the same.
6. A message indicating authentication success or failure is returned.
7. The application receives or discards the packets based on the authentication result.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 19-6** A TCP application receives packets using the keychain




# 19.3 Application Scenarios for Keychains

Keychain provides authentication for applications. The following application protocols support Keychain authentication: Routing Information Protocol (RIP), Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Multicast Source Discovery Protocol (MSDP). Applications use the same Keychain authentication procedures. Create a Keychain and then use the Keychain to perform an authentication.

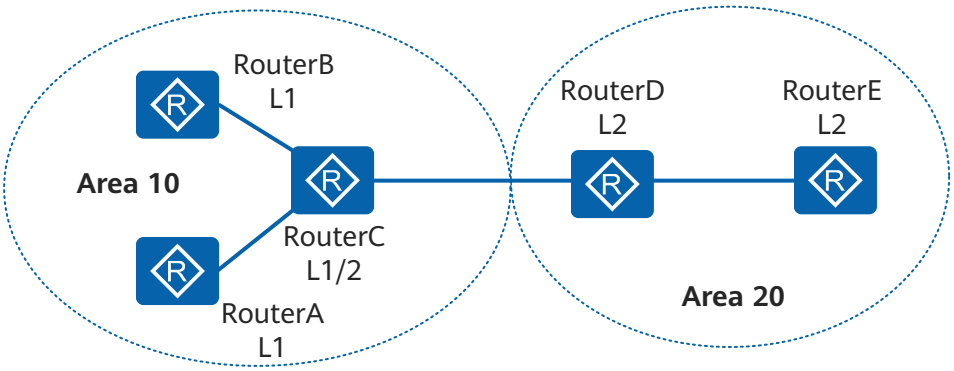
## IS-IS Using Keychain for Authentication

IS-IS is a commonly used routing protocol, and IS-IS security is needed. You can configure a fixed authentication algorithm and key to authenticate IS-IS packets. But fixed authentication algorithms and keys may be decrypted. The use of Keychain to authenticate the IS-IS packets makes IS-IS more secure.

As shown in **Figure 19-7**, Router A, Router B, Router C, Router D, and Router E use IS-IS to communicate. Router A, Router B, and Router C belong to area 10; Router D and Router E belong to area 20. Router A and Router B are Level-1 devices; Router D and Router E are Level-2 devices; Router C is a Level-1-2 device. Create a Keychain on each device to authenticate the IS-IS packets. Configure area and domain authentication in the IS-IS process, and configure interface authentication on the interface as well.

 Copyright © Huawei Technologies Co., Ltd. 

**Figure 19-7** IS-IS using Keychain for authentication




# 19.4 Licensing Requirements and Limitations for Keychains

## Involved Network Elements

Other network elements are not required.

## Licensing Requirements

Keychain is a basic feature of the router and is not under license control.

## Feature Limitations

When deploying Keychain on the router, pay attention to the following:

- The keychain only manages authentication algorithms and keys and takes effect only after it is applied to an application.

The keychain supports the following protocols:

- RIP
- OSPF
- OSPFv3
- IS-IS
- MSDP
- MPLS
- BGP and BGP4+

# 19.5 Configuring a Keychain

## Pre-configuration Tasks

You can configure the keychain to periodically change authentication keys and algorithms to ensure data transmission security.

Before configuring the keychain, power on all the devices and perform self-check.

 Copyright © Huawei Technologies Co., Ltd. 

# 19.5.1 Creating a Keychain

## Context

A keychain must be created before applications are authenticated and encrypted. Deleting the keychain in use may interrupt communication. Exercise caution when you delete the keychain.

Transmission Control Protocol (TCP) applications are connected using TCP authentication. TCP uses enhanced TCP authentication options to send TCP authentication packets. Vendors use different *kind-value*s to represent the enhanced TCP authentication option and different IDs to represent different algorithms. When a keychain is applied to a TCP application, you must configure the kind value and the mapping between the TCP algorithm and algorithm ID based on the peer configuration so that devices of different vendors can communicate.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **keychain** *keychain-name* **mode** { **absolute** | **periodic** { **daily** | **weekly** | **monthly** | **yearly** } }

A keychain is created and the keychain view is displayed.

**Step 3** (Optional) Configure parameters in TCP authentication.

1. Run **tcp-kind** *kind-value*

   The TCP type value of the keychain is configured.

2. Run **tcp-algorithm-id** { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** } *algorithm-id*

   The mapping between the TCP algorithm and algorithm ID is configured.

   NOTE

   HMAC-MD5 and MD5 have potential security risks. HMAC-SHA-256 or SHA-256 is recommended.

**Step 4** (Optional) Run **receive-tolerance** { *value* | **infinite** }

The receive tolerance time is configured.

NOTE

You are advised to set the receive tolerance time to advance the start receive time and delay the end receive time so that packets are not lost due to time asynchronization on the network.

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

# 19.5.2 Configuring a Key

## Context

A key is the authentication rule of a keychain. A key includes an algorithm, a key string, active send time, active receive time, and the key status. A keychain supports a maximum of 64 keys.

There is only one key ID in a keychain. Keys in different keychain may use the same key ID. Only one send key takes effect in a keychain, otherwise applications cannot determine which send key is used to encrypt packets. However, multiple receive keys may take effect in a keychain. A receive key that has the same key ID with the receiving packet is used for decryption.

If the key on the sending end changes, the key on the receiving end also needs to be changed. A delay may occur when the receiving end and the sending end change keys due to time asynchronization on the network. Packets may be lost during the delay. The receive tolerance time can be configured to prevent packet loss during the key change. The receive tolerance time only takes effect on keys on the receiving end. The receive tolerance time advances the start receive time and delays the end receive time.

If no key is configured in a period, no send key is active in that period. Therefore, applications do not send authentication packets to each other. A default send key can be configured to prevent this situation. All keys can be specified as the default send key. A keychain has only one default send key. When no other send keys are active, the default send key takes effect.

## Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **keychain** *keychain-name*

The keychain view is displayed.

**Step 3** (Optional) Run **time mode** { **utc** | **lmt** }

The time mode for keychain is configured.

**Step 4** Run **key-id** *key-id*

A key-id is configured and the key-id view is displayed to configure a key.

**Step 5** Run **algorithm** { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** | **simple** }

An algorithm is configured.

Different protocols support different algorithms.

RIP supports MD5 and simple. BGP and BGP4+ support MD5. IS-IS supports MD5 and simple. OSPF supports MD5, simple and hmac-md5. MSDP supports MD5. MPLS LDP supports MD5. MPLS TE supports HMAC-MD5.

 Copyright © Huawei Technologies Co., Ltd. 

NOTE

HMAC-MD5 and MD5 have potential security risks. HMAC-SHA-256 or SHA-256 is recommended.

The authentication algorithm specified by **simple** is not secure. HMAC-SHA-256 or SHA-256 is recommended.

**Step 6** Run **key-string** { **plain** *plain-text* | [ **cipher** ] *cipher-text* }

A key string is configured.

NOTE

When configuring an authentication password, select the ciphertext mode because the password is saved in the configuration file as a simple text if you select the plaintext mode, which has a high risk. To ensure device security, change the password periodically.

**Step 7** Configure the send time. Different time modes use different commands to configure the send time. **Table 19-1** shows commands to configure the send time based on different time modes.

**Table 19-1** Configuring the send time

| Time Mode | Command to Configure the Send Time |
| --- | --- |
| **absolute** | **send-time** *start-time start-date* { **duration** { *duration-value* \| **infinite** } \| **to** *end-time end-date* } |
| **periodic daily** | **send-time daily** *start-time* **to** *end-time* |
| **periodic weekly** | **send-time day** { *start-day-name* **to** *end-day-name* \| *day-name &<1-7>* } |
| **periodic monthly** | **send-time date** { *start-date-value* **to** *end-date-value* \| *date-value &<1-31>* } |
| **periodic yearly** | **send-time month** { *start-month-name* **to** *end-month-name* \| *month-name &<1-12>* } |

NOTE

You are advised to enable network time protocol (NTP) to keep time consistency.

**Step 8** Configure the receive time. Different time modes use different commands to configure the receive time. **Table 19-2** shows commands to configure the receive time based on different time modes.

**Table 19-2** Configure the receive time

| Time Mode | Command to Configure Receive Time |
| --- | --- |
| **absolute** | **receive-time** *start-time start-date* { **duration** { *duration-value* \| **infinite** } \| **to** *end-time end-date* } |

 Copyright © Huawei Technologies Co., Ltd. 

| Time Mode | Command to Configure Receive Time |
| --- | --- |
| **periodic daily** | **receive-time daily** *start-time* **to** *end-time* |
| **periodic weekly** | **receive-time day** { *start-day-name* **to** *end-day-name* \| *day-name &<1-7>* } |
| **periodic monthly** | **receive-time date** { *start-date-value* **to** *end-date-value* \| *date-value &<1-31>* } |
| **periodic yearly** | **receive-time month** { *start-month-name* **to** *end-month-name* \| *month-name &<1-12>* } |

**Step 9** (Optional) Run **default send-key-id**

The key is configured as the default key for sending packets.

**----End**

## 19.5.3 Applying the Keychain

### Context

The keychain only takes effect after it is applied to an application.

This section uses RIP as an example to describe how to apply the keychain to applications. Different applications may use different commands to apply the Keychain. **Table 19-3** lists the commands used by different applications.

**Table 19-3** Protocols that support the keychain authentication

| Protocol | Link |
| --- | --- |
| RIP | **rip authentication-mode** |
| MSDP | **peer keychain (MSDP)** |
| OSPF | **authentication-mode (OSPF)**<br>**ospf authentication-mode** |
| IS-IS | **area-authentication-mode**<br>**isis authentication-mode** |
| BGP\BGP4+ | **peer keychain (BGP)** |
| MPLS LDP | **authentication key-chain** |
| MPLS RSVP | **mpls rsvp-te authentication** |


Copyright © Huawei Technologies Co., Ltd.

### Procedure

**Step 1** Run **system-view**

The system view is displayed.

**Step 2** Run **interface** *interface-type interface-number*

The interface view is displayed.

**Step 3** Run **rip authentication-modekeychain** *keychain-name*

The keychain used by RIP is configured.

**----End**

## 19.5.4 Verifying the Keychain Configuration

### Procedure

- Run the **display keychain** *keychain-name* command to check the keychain configuration.
- Run the **display keychain** *keychain-name* **key-id** *key-id* command to check the key-id configuration.

**----End**

# 19.6 Configuration Examples for Keychains

## 19.6.1 Example for Applying the Keychain to RIP

### Networking Requirements

As shown in **Figure 19-8**, RouterA and RouterB are connected using RIP-2.

The RIP connection needs to be retained during data transmission.

**Figure 19-8** Networking diagram of applying the keychain to RIP




### Configuration Roadmap

To ensure stable RIP connections, RIP protocol packets must be correctly transmitted. You are advised to authenticate and encrypt the packets to ensure transmission security. In addition, to prevent unauthorized users from forging algorithms and key strings used in authentication and encryption, you are advised to dynamically change algorithms and key strings to ensure secure RIP packet transmission. Therefore, the keychain protocol is used to ensure stability of RIP connections.

 Copyright © Huawei Technologies Co., Ltd. 

The configuration roadmap is as follows:

1. Configure basic RIP functions.
2. Configure a keychain.
3. Apply the keychain to RIP.

## Procedure

**Step 1** Configure basic RIP functions.

# Configure Router A.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] rip 1
[RouterA-rip-1] version 2
[RouterA-rip-1] network 192.168.1.0
[RouterA-rip-1] quit
```

# Configure Router B.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] rip 1
[RouterB-rip-1] version 2
[RouterB-rip-1] network 192.168.1.0
[RouterB-rip-1] quit
```

**Step 2** Configure a keychain.

# Configure Router A.

```
[RouterA] keychain huawei mode absolute
[RouterA-keychain-huawei] receive-tolerance 100
[RouterA-keychain-huawei] key-id 1
[RouterA-keychain-huawei-keyid-1] algorithm sha-256
[RouterA-keychain-huawei-keyid-1] key-string cipher Huawei@1234
[RouterA-keychain-huawei-keyid-1] send-time 0:00 2012-3-12 to 23:59 2012-3-12
[RouterA-keychain-huawei-keyid-1] receive-time 0:00 2012-3-12 to 23:59 2012-3-12
[RouterA-keychain-huawei-keyid-1] default send-key-id
[RouterA-keychain-huawei-keyid-1] quit
[RouterA-keychain-huawei] quit
```

# Configure Router B.

```
[RouterB] keychain huawei mode absolute
[RouterB-keychain-huawei] receive-tolerance 100
[RouterB-keychain-huawei] key-id 1
[RouterB-keychain-huawei-keyid-1] algorithm sha-256
[RouterB-keychain-huawei-keyid-1] key-string cipher Huawei@1234
[RouterA-keychain-huawei-keyid-1] send-time 0:00 2012-3-12 to 23:59 2012-3-12
[RouterA-keychain-huawei-keyid-1] receive-time 0:00 2012-3-12 to 23:59 2012-3-12
[RouterB-keychain-huawei-keyid-1] default send-key-id
[RouterB-keychain-huawei-keyid-1] quit
[RouterB-keychain-huawei] quit
```

**Step 3** Apply the keychain to RIP.

# Configure Router A.

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet1/0/0] rip authentication-mode keychain huawei
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] quit
```

# Configure Router B.

 Copyright © Huawei Technologies Co., Ltd. 

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 192.168.1.2 24
[RouterB-GigabitEthernet1/0/0] rip authentication-mode keychain huawei
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] quit
```

**Step 4** Verify the configuration.

# Run the **display keychain** *keychain-name* command to check the key-id status of the keychain.

```
<RouterA> display keychain huawei
 Keychain Information:
 ----------------------
 Keychain Name            : huawei
   Timer Mode             : Absolute
   Receive Tolerance(min)  : 100
   TCP Kind               : 254
   TCP Algorithm IDs      :
     HMAC-MD5             : 5
     HMAC-SHA1-12         : 2
     HMAC-SHA1-20         : 6
     HMAC-SHA-256         : 7
     SHA-256              : 8
     MD5                  : 3
     SHA1                 : 4
 Number of Key IDs        : 1
 Active Send Key ID       : 1
 Active Receive Key IDs   : 01
 Default send Key ID      : Not configured

 Key ID Information:
 ----------------------
 Key ID                   : 1
   Key string             : ******
   Algorithm              : SHA-256
   SEND TIMER             :
     Start time           : 2012-03-12 00:00
     End time             : 2012-03-12 23:59
     Status               : Active
   RECEIVE TIMER          :
     Start time           : 2012-03-12 00:00
     End time             : 2012-03-12 23:59
     Status               : Active
```

# After the keychain is applied to RIP, run the **display rip** *process-id* **interface verbose** command to check the authentication mode of RIP packets. The display on Router A is used as an example.

```
<RouterA> display rip 1 interface verbose
 GigabitEthernet1/0/0(192.168.1.1)
  State          : UP          MTU    : 500
  Metricin       : 0
  Metricout      : 1
  Input          : Enabled     Output : Enabled
  Protocol       : RIPv2 Multicast
  Send version   : RIPv2 Multicast Packets
  Receive version : RIPv2 Multicast and Broadcast Packets
  Poison-reverse              : Disabled
  Split-Horizon               : Enabled
  Authentication type         : MD5 (Non-standard - Keychain: huawei)
    Last Sequence Number Sent  : 0x0
  Replay Protection           : Disabled
```

**----End**

 Copyright © Huawei Technologies Co., Ltd. 

## Configuration Files

- Router A configuration file

```
#
 sysname RouterA
#
keychain huawei mode absolute
 receive-tolerance 100
 key-id 1
  algorithm sha-256
  key-string cipher %#%#e7,_2i0MfN6W5@Fb6Q3WU.\e)ju5"Jr&&())JmZ2%#%#
  send-time 00:00 2012-03-12 to 23:59 2012-03-12
  receive-time 00:00 2012-03-12 to 23:59 2012-03-12
  default send-key-id
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
 rip authentication-mode keychain huawei
#
rip 1
 version 2
 network 192.168.1.0
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
keychain huawei mode absolute
 receive-tolerance 100
 key-id 1
  algorithm sha-256
  key-string cipher %#%#e7,_2i0MfN6W5@Fb6Q3WU.\e)ju5"Jr&&())JmZ2%#%#
  send-time 00:00 2012-03-12 to 23:59 2012-03-12
  receive-time 00:00 2012-03-12 to 23:59 2012-03-12
  default send-key-id
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
 rip authentication-mode keychain huawei
#
rip 1
 version 2
 network 192.168.1.0
#
return
```

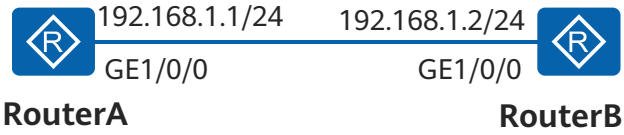
# 19.6.2 Example for Applying the Keychain to BGP

## Networking Requirements

As shown in **Figure 19-9**, RouterA and RouterB are connected using BGP.

The BGP connection needs to be retained during data transmission.

**Figure 19-9** Networking diagram of applying the keychain to BGP




 Copyright © Huawei Technologies Co., Ltd. 

## Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the basic keychain functions.
2. Configure a keychain for Router to authenticate BGP.

## Procedure

**Step 1** Configure a keychain.

# Configure Router A.

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] keychain huawei mode periodic weekly
[RouterA-keychain-huawei] tcp-kind 182
[RouterA-keychain-huawei] tcp-algorithm-id sha-256 17
[RouterA-keychain-huawei] receive-tolerance 100
[RouterA-keychain-huawei] key-id 1
[RouterA-keychain-huawei-keyid-1] algorithm sha-256
[RouterA-keychain-huawei-keyid-1] key-string cipher Huawei@1234
[RouterA-keychain-huawei-keyid-1] send-time day fri sat
[RouterA-keychain-huawei-keyid-1] receive-time day fri sat
[RouterA-keychain-huawei-keyid-1] default send-key-id
[RouterA-keychain-huawei-keyid-1] quit
[RouterA-keychain-huawei] quit
```

# Configure Router B.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] keychain huawei mode periodic weekly
[RouterB-keychain-huawei] tcp-kind 182
[RouterB-keychain-huawei] tcp-algorithm-id sha-256 17
[RouterB-keychain-huawei] receive-tolerance 100
[RouterB-keychain-huawei] key-id 1
[RouterB-keychain-huawei-keyid-1] algorithm sha-256
[RouterB-keychain-huawei-keyid-1] key-string cipher Huawei@1234
[RouterB-keychain-huawei-keyid-1] send-time day fri sat
[RouterB-keychain-huawei-keyid-1] receive-time day fri sat
[RouterB-keychain-huawei-keyid-1] default send-key-id
[RouterB-keychain-huawei-keyid-1] quit
[RouterB-keychain-huawei] quit
```

**Step 2** Apply the keychain to BGP for authentication and encryption.

# Configure Router A.

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
[RouterA] bgp 1
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 192.168.1.2 as-number 1
[RouterA-bgp] peer 192.168.1.2 keychain huawei
[RouterA-bgp] quit
[RouterA] quit
```

# Configure Router B.

```
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 192.168.1.2 24
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] bgp 1
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 192.168.1.1 as-number 1
```

 Copyright © Huawei Technologies Co., Ltd. 

```
[RouterB-bgp] peer 192.168.1.1 keychain huawei
[RouterB-bgp] quit
[RouterB] quit
```

**Step 3** Verify the configuration.

# Run the **display keychain** *keychain-name* command to check the key-id status of the keychain.

```
<RouterA> display keychain huawei
 Keychain Information:
 ----------------------
 Keychain Name            : huawei
   Timer Mode             : Weekly periodic
   Receive Tolerance(min)  : 100
   TCP Kind               : 182
   TCP Algorithm IDs      :
     HMAC-MD5             : 5
     HMAC-SHA1-12         : 2
     HMAC-SHA1-20         : 6
     HMAC-SHA-256         : 7
     SHA-256              : 17
     MD5                  : 8
     SHA1                 : 4
 Number of Key IDs        : 1
 Active Send Key ID       : 1
 Active Receive Key IDs    : 01
 Default send Key ID      : Not configured


 Key ID Information:
 -------------------
 Key ID                   : 1
   Key string             : ******
   Algorithm              : SHA-256
   SEND TIMER             :
     Day(s)               : Fri Sat
     Status               : Active
   RECEIVE TIMER          :
     Day(s)               : Fri Sat
     Status               : Active
```

# After the keychain is applied to BGP, run the **display bgp peer** *ipv4-address* **verbose** command to check authentication information about the BGP peer. The display on Router A is used as an example.

```
<RouterA> display bgp peer 192.168.1.2 verbose
      BGP Peer is 192.168.1.2,  remote AS 1
      Type: IBGP link
      BGP version 4, Remote router ID 2.2.2.2
      Update-group ID: 1
      BGP current state: Established, Up for 00h43m34s
      BGP current event: RecvKeepalive
      BGP last state: OpenConfirm
      BGP Peer Up count: 1
      Received total routes: 0
      Received active routes total: 0
      Received mac routes: 0
      Advertised total routes: 0
      Port:  Local - 179      Remote - 55828
      Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
      Received  : Active Hold Time: 180 sec
      Negotiated: Active Hold Time: 180 sec   Keepalive Time:60 sec
      Peer optional capabilities:
      Peer supports bgp multi-protocol extension
      Peer supports bgp route refresh capability
      Peer supports bgp 4-byte-as capability
      Address family IPv4 Unicast: advertised and received
Received: Total 45 messages
```

 Copyright © Huawei Technologies Co., Ltd. 

```
            Update messages              0
            Open messages                1
            KeepAlive messages           44
            Notification messages        0
            Refresh messages             0
Sent: Total 48 messages
            Update messages              0
            Open messages                2
            KeepAlive messages           46
            Notification messages        0
            Refresh messages             0
Authentication type configured: Keychain(huawei)
Last keepalive received: 2012/04/20 11:37:27
Last keepalive sent    : 2012/04/20 11:37:27
Minimum route advertisement interval is 15 seconds
Optional capabilities:
Route refresh capability has been enabled
4-byte-as capability has been enabled
Peer Preferred Value: 0
Routing policy configured:
No routing policy is configured
```

**----End**

## Configuration Files

- Router A configuration file

```
#
 sysname RouterA
#
keychain huawei mode periodic weekly
 receive-tolerance 100
 tcp-kind 182
 tcp-algorithm-id sha-256 17
 key-id 1
  algorithm sha-256
  key-string cipher %#%#j8P<=eo2u$q}YxHvZ/"8M:=n!+K>xX1;D~L'`d78%#%#
  send-time day fri sat
  receive-time day fri sat
  default send-key-id
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
#
bgp 1
 router-id 1.1.1.1
 peer 192.168.1.2 as-number 1
 peer 192.168.1.2 keychain huawei
 #
 ipv4-family unicast
  undo synchronization
  peer 192.168.1.2 enable
#
return
```

- Configuration file of Router B

```
#
 sysname RouterB
#
keychain huawei mode periodic weekly
 receive-tolerance 100
 tcp-kind 182
 tcp-algorithm-id sha-256 17
 key-id 1
  algorithm sha-256
  key-string cipher %#%#j8P<=eo2u$q}YxHvZ/"8M:=n!+K>xX1;D~L'`d78%#%#
  send-time day fri sat
  receive-time day fri sat
```

 Copyright © Huawei Technologies Co., Ltd. 

```
 default send-key-id
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
#
bgp 1
 router-id 2.2.2.2
 peer 192.168.1.1 as-number 1
 peer 192.168.1.1 keychain huawei
 #
 ipv4-family unicast
  undo synchronization
  peer 192.168.1.1 enable
#
return
```