21 Network Management and Monitoring Commands

About This Chapter

21.1 SNMP Configuration Commands
21.2 RMON and RMON2 Configuration Commands
21.3 TCP FPM Configuration Commands
21.4 IP FPM Configuration Commands
21.5 CWMP Configuration Commands
21.6 LLDP Configuration Commands
21.7 NQA Configuration Commands
21.8 LSDP Configuration Commands
21.9 Service Diagnosis Configuration Commands
21.10 Mirroring Configuration Commands
21.11 Packet Capture Configuration Command
21.12 NetStream Configuration Commands
21.13 IP Accounting Configuration Commands
21.14 TWAMP Light Configuration Commands
21.15 Ping and Tracert Configuration Commands

21.1 SNMP Configuration Commands

NOTE

AR100&AR120 series (except AR129CV&AR129CVW&AR129CGVW-L) do not support SNMP.

 Copyright © Huawei Technologies Co., Ltd.

21.1.1 display snmp-agent community

Function

The **display snmp-agent community** command displays the configured community name.

Format

display snmp-agent community { **read** | **write** }

Parameters

Parameter	Description	Value
read	Displays the name of a read-only community. The parameter is specified using the **snmp-agent community** command.	-
write	Displays the name of a read-write community. The parameter is specified using the **snmp-agent community** command.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

When configuring a management entity, you can use the **display snmp-agent community** command to check the community name configured on the current agent.

You have to configure the community name using the **snmp-agent community** command before you run the **display snmp-agent community** command.

Example

Display the current community name.

```
<Huawei> display snmp-agent community read
  Community name: %@%@$X!5#d+t+OJOXL1[{O2!&Fe&0UZv'@a;R/`Y+kK$4BUGFe)&2YLuM/kMF!
HPG5Mzz3DXe2&F%@%@
  Storage type: nonVolatile
  View name: ViewDefault
  Acl: 2001

  Total number is 1
```


Copyright © Huawei Technologies Co., Ltd.

Table 21-1 Description of the display snmp-agent community read command output

Item	Description
Community name	Name of a community.
Storage type	Data storage type. The system supports the following five storage types: • volatile: Lines are saved in the volatile storage medium and are lost after the device restarts. Objects with storage type **volatile** cannot be changed to **readOnly** or **permanent**. • nonVolatile: Lines are saved in the nonvolatile storage medium such as Non Volatile Random Access Memory (NVRAM) and can be restored after the device restarts. Objects with storage type **nonVolatile** cannot be changed to **readOnly** or **permanent**. • permanent: Permanent lines are saved in the nonvolatile storage medium such as Read-only Memory (ROM). They can be modified but cannot be deleted. Rowstatus objects with storage type **permanent** cannot be modified. • readOnly: Read-only lines are saved in the nonvolatile storage medium such as ROM. They cannot be modified or deleted. Rowstatus objects with storage type **readOnly** cannot be modified. • other: other storage types. In practice, the device generally uses only the **nonVolatile** type.
View name	Name of a view.
Acl	Number of the ACL configured for the community.

Related Topics

21.1.17 snmp-agent community

 Copyright © Huawei Technologies Co., Ltd.

21.1.2 display snmp-agent extend error-code status

Function

The **display snmp-agent extend error-code status** command allows you to check whether the function of sending extended error codes to the NMS is enabled on the device.

Format

display snmp-agent extend error-code status

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

If the NMS does not receive the extended error codes sent from the device, you can run the **display snmp-agent extend error-code status** command to check whether the function of sending extended error codes is enabled on the device.

Example

Display whether the function of sending extended error codes is enabled on the device.

```
<Huawei> display snmp-agent extend error-code status
Extend error-code status: enabled
```

Table 21-2 Description of the display snmp-agent extend error-code status command output

Item	Description
Extend error-code status	Whether the function of sending extended error codes is enabled. • enabled: The function of sending extended error codes is enabled. • disabled: The function of sending extended error codes is disabled.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.20 snmp-agent extend error-code enable

21.1.3 display snmp-agent group

Function

The **display snmp-agent group** command displays information about an SNMP agent group.

Format

display snmp-agent group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays the name of an SNMP agent group.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When configuring a management object according to the SNMPv3 group information, you can run the **display snmp-agent group** command to view information about the SNMP agent group.

If the command contains no parameter, information about all groups is displayed, such as the group name, security model, and storage type.

Precautions

You can run the **display snmp-agent group** command to view information about an SNMP agent group only after the SNMP agent group is created through the **snmp-agent group** command.

Example

Display information about all SNMPv3 working groups.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display snmp-agent group

 Group name: testgroup
 Security model: v3 AuthPriv
 Readview: ViewDefault
 Writeview: dnsmib
 Notifyview: dnsmib
 Storage type: nonVolatile
 Acl: 2001

 Total number is 1
```

Table 21-3 Table 1 Description of the display snmp-agent group command output

Item	Description
Group name	Indicates the name of an SNMP agent group.
Security model	Security mode. The options are as follows: • v3 AuthPriv: authenticated and encrypted. • v3 noAuthPriv: encrypted but not authenticated. • v3 AuthnoPriv: authenticated but not encrypted. • v3 noAuthnoPriv: neither authenticated nor encrypted.
Readview	Indicates the view of the read-only MIB of the group. This parameter can be set using the **snmp-agent group** command.
Writeview	Indicates the view of the read-write MIB of the group. This parameter can be set using the **snmp-agent group** command.
Notifyview	Indicates the view of the notify MIB of the group. This parameter can be set using the **snmp-agent group** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Storage type	Data storage type. The system supports the following five storage types: • readOnly: Readonly lines are saved in the nonvolatile storage medium. They cannot be modified or deleted. Rowstatus objects with storage type **readOnly** cannot be modified. • permanent: Permanent lines are saved in the nonvolatile storage medium. They can be modified but cannot be deleted. Rowstatus objects with storage type **permanent** cannot be modified. • nonVolatile: Lines are saved in the nonvolatile storage medium and are restored after the device restarts. Objects with storage type **nonVolatile** cannot be changed to **readOnly** or **permanent**. • volatile: Lines are saved in the volatile storage medium and are lost after the device restarts. Objects with storage type **volatile** cannot be changed to **readOnly** or **permanent**. • other: other storage types. In practice, the device generally uses only the **nonVolatile** type.
Acl	Indicates the number of the ACL configured for the group.

Related Topics

21.1.21 snmp-agent group

21.1.4 display snmp-agent local-engineid

Function

The **display snmp-agent local-engineid** command displays the engine ID of the local SNMP entity.

Format

display snmp-agent local-engineid

Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The engine ID of the SNMP is the unique identity of the SNMP management feature. The engine ID uniquely identifies an SNMP entity in a management domain. The engine ID of the SNMP is one of the important components of the SNMP entity, enabling multiple functions such as message scheduling, message processing, security authentication, and access control.

After the SNMP agent function is enabled, you can run the **display snmp-agent local-engineid** command to display the default or configured local SNMP entity.

Example

Display the engine ID of the local SNMP entity.

```
<Huawei> display snmp-agent local-engineid
  SNMP local EngineID: 800007DB030819A6CDA894
```

Table 21-4 Description of the display snmp-agent local-engineid command output

Item	Description
SNMP local EngineID	The engine ID of the local SNMP entity is manually specified by an administrator using the **snmp-agent local-engineid** command or automatically generated by the system using certain algorithms.

Related Topics

21.1.22 snmp-agent local-engineid

21.1.5 display snmp-agent mib-view

Function

The **display snmp-agent mib-view** command displays the current MIB view.

Format

display snmp-agent mib-view [*view-name*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
view-name	Specifies the view to be displayed. This parameter can be set using the **snmp-agent mib-view** command.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **snmp-agent mib-view** command creates or updates a MIB view. To check the default and configured MIB view, you can run the **display snmp-agent mib-view** command.

By default, the view ViewDefault is adopted.

Precautions

Before running the **display snmp-agent mib-view** command, ensure that the SNMP agent has been enabled.

Example

Display the current MIB view.

```
<Huawei> display snmp-agent mib-view
  View name: ViewDefault
  MIB subtree: internet
  Subtree mask:
  Storage type: nonVolatile
  View type: included
  View status: active

  View name: ViewDefault
  MIB subtree: lagMIB
  Subtree mask:
  Storage type: nonVolatile
  View type: included
  View status: active

  View name: ViewDefault
  MIB subtree: snmpUsmMIB
  Subtree mask:
  Storage type: nonVolatile
  View type: excluded
  View status: active
```


Copyright © Huawei Technologies Co., Ltd.

```
View name: ViewDefault
MIB subtree: snmpVacmMIB
Subtree mask:
Storage type: nonVolatile
View type: excluded
View status: active

Total number is 1
```

Table 21-5 Description of the display snmp-agent mib-view command output

Item	Description
View name	View name.
MIB subtree	MIB subtree.
Subtree mask	Subtree mask.
Storage type	Data storage type. • volatile: Lines are saved in the volatile storage medium and are lost after the device restarts. • nonVolatile: Lines are saved in the nonvolatile storage medium and are restored after the device restarts. • permanent: Permanent lines are saved in the nonvolatile storage medium. They can be modified but cannot be deleted. • readOnly: Readonly lines are saved in the nonvolatile storage medium. They cannot be modified or deleted. • other: other storage types.
View type	Type of a view. The options are as follows: • included: The view includes the subtree. • excluded: The view excludes the subtree.
View status	Indicates the status of the MIB view.
Total number	Total number of views whose information is queried.

Related Topics

21.1.23 snmp-agent mib-view

 Copyright © Huawei Technologies Co., Ltd.

21.1.6 display snmp-agent notify-filter-profile

Function

The **display snmp-agent notify-filter-profile** command displays information about a specified trap filter profile or all trap filter profiles.

Format

display snmp-agent notify-filter-profile

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use the **display snmp-agent notify-filter-profile** command to view information about configured trap filter profiles. The command can display all the configured trap filter profiles or a specified trap file profile.

Example

Display information about configured trap filter profiles.

```
<Huawei> display snmp-agent notify-filter-profile
 Trap filter profile list:
 notify-filter name: 1
 notify-filter type: included
 notify-filter subtree: iso
 notify-filter storage-type: nonVolatile
 notify-filter status: active
```

Table 21-6 Description of the display snmp-agent notify-filter-profile command output

Item	Description
notify-filter name	Name of a trap filter profile.
notify-filter type	Whether to filter out the trap object.
notify-filter subtree	Trap filter subtree.
notify-filter storage-type	Storage mode of the trap filter profile.
notify-filter status	Status of a row.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.24 snmp-agent notify-filter-profile

21.1.7 display snmp-agent statistics

Function

The **display snmp-agent statistics** command displays statistics about SNMP messages.

Format

display snmp-agent statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display snmp-agent statistics** command analyzes the statistics about SNMP messages and obtains information about the communication between the SNMP agent and the NMS for fault location.

In an SNMP management system, the NMS and the SNMP agent exchange SNMP messages as follows:

- The NMS acts as a manager to send an SNMP Request message to the SNMP agent.
- The SNMP agent searches the MIB on the device for the required information and sends an SNMP Response message to the NMS.
- When the trap triggering conditions are met, the SNMP agent sends a trap to the NMS to report the event occurring on the device. In this manner, the network administrator can process the event occurring on the network in time.

NOTE

If large number of messages are received in short period, a great number of CPU resources are occupied. The number of received messages depends on the frequency at which the NMS sends the Request messages.

Example

Display the statistics about the SNMP messages.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display snmp-agent statistics
  The PDU process average time ( second ): 2
 0 Messages delivered to the SNMP entity
 0 Messages which were for an unsupported version
 0 Messages which used an unknown community name
 0 Messages which represented an illegal operation for the community supplied
 0 ASN.1 or BER errors in the process of decoding
 0 MIB objects retrieved successfully
 0 MIB objects altered successfully
 0 Get-request PDUs accepted and processed
 0 Get-next PDUs accepted and processed
 0 Set-request PDUs accepted and processed
 0 Messages passed from the SNMP entity
 0 Messages which were discarded, because the message queue is full
 0 SNMP PDUs which had a tooBig error (Maximum packet size 12000)
 0 SNMP PDUs which had a noSuchName error
 0 SNMP PDUs which had a had badValue error
 0 SNMP PDUs which had a general error
 0 Response PDUs accepted and processed
 0 Trap PDUs accepted and processed
 Top 10 nodes which take the longest time:
  0:PerSwitchCosttime=219ms OpType=2 OID=1.3.6.1.2.1.2.2.1.1 CallBack=0x32a51a0 CostTime=219ms
SwitchCnt=1
  1:PerSwitchCosttime=72ms OpType=2 OID=1.3.6.1.2.1.2.2.1.1 CallBack=0x32a51a0 CostTime=72ms
SwitchCnt=1
  2:PerSwitchCosttime=60ms OpType=0 OID=1.3.6.1.2.1.2.1 CallBack=0x32a3f6c CostTime=60ms
SwitchCnt=1
  3:PerSwitchCosttime=39ms OpType=0 OID=1.3.6.1.2.1.1.1 CallBack=0x32a3f6c CostTime=39ms
SwitchCnt=1
  4:PerSwitchCosttime=2ms OpType=2 OID=1.3.6.1.2.1.2.2.1.1 CallBack=0x32a51a0 CostTime=2ms
SwitchCnt=1
  5:PerSwitchCosttime=2ms OpType=2 OID=1.3.6.1.2.1.2.2.1.1 CallBack=0x32a51a0 CostTime=2ms
SwitchCnt=1
  6:PerSwitchCosttime=2ms OpType=2 OID=1.3.6.1.2.1.2.2.1.1 CallBack=0x32a51a0 CostTime=2ms
SwitchCnt=1
  7:PerSwitchCosttime=2ms OpType=2 OID=1.3.6.1.2.1.2.2.1.2 CallBack=0x32a51a0 CostTime=2ms
SwitchCnt=1
  8:PerSwitchCosttime=2ms OpType=2 OID=1.3.6.1.2.1.2.2.1.2 CallBack=0x32a51a0 CostTime=2ms
SwitchCnt=1
  9:PerSwitchCosttime=1ms OpType=0 OID=1.3.6.1.2.1.1.2 CallBack=0x32a3f6c CostTime=1ms SwitchCnt=1
```

Table 21-7 Description of the display snmp-agent statistics command output

Item	Description
Messages delivered to the SNMP entity	Total number of received SNMP messages.
Messages which were for an unsupported version	Number of messages with incorrect version information.
Messages which used an unknown community name	Number of messages with incorrect community names.
Messages which represented an illegal operation for the community supplied	Number of messages whose community names have incorrect access rights.
ASN.1 or BER errors in the process of decoding	Number of SNMP messages with encoding errors.
MIB objects retrieved successfully	Number of variables requested by the NMS.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
MIB objects altered successfully	Number of variables set by the NMS.
Get-request PDUs accepted and processed	Number of received GetRequest messages.
Get-next PDUs accepted and processed	Number of received GetNextRequest messages.
Set-request PDUs accepted and processed	Number of received SetRequest messages.
Messages passed from the SNMP entity	Total number of outgoing SNMP messages.
Messages which were discarded, because the message queue is full	Total number of discarded SNMP messages resulting in an outbound message queue being full.
SNMP PDUs which had a tooBig error (Maximum packet size 12000)	Number of SNMP messages with Too_big errors.
SNMP PDUs which had a noSuchName error	Number of messages with noSuchName errors.
SNMP PDUs which had a had badValue error	Number of SNMP messages with Bad_values errors.
SNMP PDUs which had a general error	Number of SNMP messages with General_errors.
Response PDUs accepted and processed	Number of received response messages.
Trap PDUs accepted and processed	Number of sent traps.
NOTE V200R010C10 and later versions support the following parameters.	
Top 10 nodes which take the longest time	Top 10 objects that take the longest time to complete.
PerSwitchCosttime	Time consumed before a single handover.
OpType	Operation type.
OID	OID.
CallBack	Callback address.
CostTime	Total time consumed.
SwitchCnt	Number of switchovers.

Copyright © Huawei Technologies Co., Ltd.

21.1.8 display snmp-agent sys-info

Function

The **display snmp-agent sys-info** command displays the system information of the current SNMP device, including the contact information about the system maintenance, physical location of the device, and SNMP version.

Format

display snmp-agent sys-info [**contact** | **location** | **version**] *

Parameters

Parameter	Description	Value
contact	Displays the contact information of the current SNMP device.	-
location	Displays the physical location information of the current SNMP device.	-
version	Displays the SNMP version running in the current system.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use the **display snmp-agent sys-info** command to check the system maintenance information of the current SNMP device. The information includes:

- Contact information of the device administrator
- Physical location of the device
- SNMP version

If the parameter is not specified, all information is displayed.

The **snmp-agent sys-info** command can be used to set the output of the **display snmp-agent sys-info** command

Example

Display the system information of the SNMP agent.

```
<Huawei> display snmp-agent sys-info
 The contact person for this managed node:
        R&D Beijing, Huawei Technologies Co.,Ltd.
  The physical location of this node:
        Beijing China
  SNMP version running in the system:
        SNMPv2c
```


Copyright © Huawei Technologies Co., Ltd.

Display the SNMP version running in the current system.

```
<Huawei> display snmp-agent sys-info version
  SNMP version running in the system:
        SNMPv2c
```

Display the contact information of the current SNMP device.

```
<Huawei> display snmp-agent sys-info contact
 The contact person for this managed node:
        R&D Beijing, Huawei Technologies Co.,Ltd.
```

Display the physical location information of the current SNMP device.

```
<Huawei> display snmp-agent sys-info location
 The physical location of this node:
        Beijing China
```

Table 21-8 Description of the display snmp-agent sys-info command output

Item	Description
The contact person for this managed node:	Contact person of the managed device. By specifying this parameter, you can store the important information to the router for convenient query.
The physical location of this node:	Location of the managed device.
SNMP version running in the system:	SNMP version running in the current system. The value can be: • SNMPv1 • SNMPv2c • SNMPv3

Related Topics

21.1.26 snmp-agent sys-info

21.1.9 display snmp-agent target-host

Function

The **display snmp-agent target-host** command displays the list of destination hosts that receive traps.

Format

display snmp-agent target-host

Parameters

None

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use this command to query the IP addresses of all valid destination hosts that are configured to receive traps. The command output consists of the following two parts:

- List of the destination hosts that receive traps.
- Parameter list of the destination hosts and hosts that are not bound to the parameters.

Precautions

Host parameters must have been configured for the destination host. Otherwise, the destination host cannot receive traps, and parameters are not displayed.

Example

Display the configurations of all destination hosts in the system.

```
<Huawei> 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: SNMPV3
  Trap version of the target host: v3
  Security name of the target host:  %@%@_=XqAFC_94uCS,3'<gYC*ZU6%@%@
  Security level of the target host: privacy

  Total number is 1
```

Table 21-9 Description of the display snmp-agent target-host command output

Item	Description
Traphost list	List of the destination hosts that receive traps.
Target host name	Name of a destination host that receives traps.
Traphost address	IP address of a destination host that receives traps.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Traphost portnumber	Number of the port on a destination host for receiving traps.
Target host parameter	Parameter name of a destination host that receives traps.
Parameter list trap target host	Parameter list of destination hosts that receive traps.
Parameter name of the target host	Parameter name of destination hosts that receive traps.
Message mode of the target host	Protocol used by destination hosts that receive traps.
Trap version of the target host	Version of the protocol for transmitting traps.
Security name of the target host	Security name of destination hosts that receive traps.
Security level of the target host	Authentication mode of traps.
Total number	Total number of views whose information is queried.

Related Topics

21.1.30 snmp-agent trap enable

21.1.10 display snmp-agent trap all

Function

The **display snmp-agent trap all** command checks current and default status of all traps in all features.

Format

display snmp-agent trap [**feature-name** *feature-name*] **all**

Parameters

Parameter	Description	Value
feature-name *feature-name*	Specifies a feature that generates traps.	-

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

After the device is enabled to send traps to the NMS:

- You can run the **display snmp-agent trap all** command to check the status of all traps in all features.
- You can run the **display snmp-agent trap feature-name** *feature-name* **all** command to check the status of all traps in a specified feature.

Example

Check the default status of all traps in all features.

```
<Huawei> display snmp-agent trap all
------------------------------------------------------------------------------
Feature name: SSH
Trap number : 1
------------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
hwSSHSftpUserNumExceedMax      off                     off
------------------------------------------------------------------------------
Feature name: VFS
Trap number : 3
------------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
hwFlhOperNotification          off                     off
hwFlhSyncSuccessNotification   off                     off
hwFlhSyncFailNotification      off                     off
------------------------------------------------------------------------------
  ---- More ----
```

Table 21-10 Description of the display snmp-agent trap all command output

Item	Description
Feature name	Name of the feature that generates traps.
Trap number	Number of traps generated by this feature.
Trap name	Trap name.
Default switch status	Default status of the trap function: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current switch status	Current status of the trap function: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

21.1.29 snmp-agent trap disable

21.1.30 snmp-agent trap enable

21.1.31 snmp-agent trap enable feature-name

21.1.11 display snmp-agent trap feature-name snmp all

Function

The **display snmp-agent trap feature-name snmp all** command displays whether all SNMP traps are enabled.

Format

display snmp-agent trap feature-name snmp all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display snmp-agent trap feature-name snmp all** command to check status of all SNMP traps. This status can be configured using the **snmp-agent trap enable feature-name snmp** command.

Example

View whether all SNMP traps are enabled.

```
<Huawei>display snmp-agent trap feature-name snmp all
------------------------------------------------------------------------------
Feature name: SNMP
Trap number : 3
```


Copyright © Huawei Technologies Co., Ltd.

```
-------------------------------------------------------------------------------
Trap name                Default switch status   Current switch status
coldStart                on                      on
warmStart                on                      on
authenticationFailure    off                     off
```

Table 21-11 Description of the display snmp-agent trap feature-name snmp all command output

Item	Description
Feature name	Name of the module where the trap is generated
Trap number	Number of traps.
Trap name	Name of trap, including • authenticationFailure: This trap is generated when a user uses an incorrect community name and is unable to log in to the device. • coldStart: This trap is generated when the device is powered off and restarted. • warmStart: This trap is generated when the status of SNMP agent is changed from disable to enable.
Default switch status	Default status of a trap • on: The trap function is enabled. • off: The trap function is disabled.
Current switch status	Current status of a trap • on: The trap function is enabled. • off: The trap function is disabled. This status can be configured using the **snmp-agent trap enable feature-name snmp** command.

Related Topics

21.1.32 snmp-agent trap enable feature-name snmp

21.1.12 display snmp-agent trap-source

Function

The **display snmp-agent trap-source** command displays the source interface that sends trap messages.

Format

display snmp-agent trap-source

Parameters

None

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

After users run the **snmp-agent trap source** command to configure the source interface that sends trap messages, you can run the **display snmp-agent trap-source** command to display the configured source interface.

Example

Display the source interface that sends trap messages.

```
<Huawei> display snmp-agent trap-source
  Trap source interface name: GigabitEthernet1/0/0
```

Table 21-12 Description of the display snmp-agent trap-source output

Item	Description
Trap source interface name	Source interface that sends trap messages.

Related Topics

21.1.36 snmp-agent trap source

21.1.13 display snmp-agent usm-user

Function

The **display snmp-agent usm-user** command displays information about an SNMPv3 user.

Format

display snmp-agent usm-user [*user-name*]

Parameters

Parameter	Description	Value
user-name	Specifies an SNMPv3 user. This parameter is specified using the **snmp-agent usm-user** command.	-

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The displayed information about an SNMPv3 user includes:

- User name.
- Local engine ID of the user. The SNMPv3 engine ID uniquely identifies an SNMPv3 agent in a management domain. The SNMPv3 engine ID is an important component of the SNMPv3 agent. It schedules and processes SNMPv3 messages, and implements security authentication and access control.

Precautions

The **display snmp-agent usm-user** command is applicable only to SNMPv3 users.

Example

Display information about all current SNMPv3 users.

```
<Huawei> display snmp-agent usm-user
  User name: testuser
  Engine ID: 800007DB03548998F3A458
  Group name: testgroup
  Authentication mode: md5, Privacy mode: des56
  Storage type: nonVolatile
  User status: active

  Total number is 1
```

Table 21-13 Description of the display snmp-agent usm-user command output

Item	Description
User name	SNMPv3 user name, which identifies a user.
Engine ID	Engine ID corresponding to the SNMPv3 user.
Group name	SNMPv3 group name corresponding to the SNMPv3 user.
Authentication mode	Authentication mode for the SNMPv3 user: • md5 • No authentication mode

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Privacy mode	Encryption mode for the SNMPv3 user: • des56 • aes128
Storage type	Data storage type. • volatile: Lines are saved in the volatile storage medium and are lost after the device restarts. • nonVolatile: Lines are saved in the nonvolatile storage medium and are restored after the device restarts. • permanent: Permanent lines are saved in the nonvolatile storage medium. They can be modified but cannot be deleted. • readOnly: Readonly lines are saved in the nonvolatile storage medium. They cannot be modified or deleted. • other: other storage types.
User status	Status of the SNMPv3 user: • active • inactive
Total number	Number of SNMPv3 users.

Related Topics

21.1.21 snmp-agent group

21.1.22 snmp-agent local-engineid

21.1.37 snmp-agent usm-user

21.1.14 enable snmp trap updown

Function

The **enable snmp trap updown** command enables an interface to send a trap to the NMS when the protocol status of the interface changes.

The **undo enable snmp trap updown** command disables an interface from sending a trap to the NMS when the protocol status of the interface changes.

By default, an interface sends a Trap message to the NMS when the protocol status of the interface changes.

Copyright © Huawei Technologies Co., Ltd.

Format

enable snmp trap updown

undo enable snmp trap updown

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **enable snmp trap updown** command is used to enable an interface to send a Trap message to the NMS when the protocol status of the interface changes, which helps the NMS monitor the interface status in real time.

Precautions

By default, the function of sending a Trap message to the NMS when the protocol status of the interface changes is enabled. If an interface alternates between Up and Down, it will frequently send Trap messages to the NMS, causing the NMS to be busy processing these Trap messages. In this case, you can run the **undo enable snmp trap updown** command to disable the interface from sending trap messages to the NMS.

Example

Enable an interface to send a trap to the NMS when the protocol status of the interface changes.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] enable snmp trap updown
```

21.1.15 snmp-agent

Function

The **snmp-agent** command enables the SNMP agent function.

The **undo snmp-agent** command disables the SNMP agent function.

By default, the SNMP agent function is disabled.

Format

snmp-agent

Copyright © Huawei Technologies Co., Ltd.

undo snmp-agent

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By executing the **snmp-agent** command with any parameter enables the SNMP agent function. For example, if you execute the **snmp-agent community** command, the community name gets created and also SNMP agent function is enabled.

Precautions

- To configure SNMP functions using the command, you do not need to run the **snmp-agent** command to enable the SNMP agent function.
- To configure SNMP functions using the configuration file, you need to run the **snmp-agent** command in the configuration file; otherwise, you cannot enable SNMP functions.

Example

Enable the SNMP agent function.

```
<Huawei> system-view
[Huawei] snmp-agent
```

Disable the SNMP agent function.

```
<Huawei> system-view
[Huawei] undo snmp-agent
```

21.1.16 snmp-agent bulk-fast enable

Function

The **snmp-agent bulk-fast enable** command enables the function of accelerating the SNMP GetBulk operation.

The **undo snmp-agent bulk-fast enable** command disables the function of accelerating the SNMP GetBulk operation.

By default, the function of accelerating the SNMP GetBulk operation is disabled.

Copyright © Huawei Technologies Co., Ltd.

NOTE

This function is supported in V200R010C10 and later versions.

Format

snmp-agent bulk-fast enable

undo snmp-agent bulk-fast enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

The GetBulk operation is slow when only some SNMP views are configured. You can run the **snmp-agent bulk-fast enable** command to enable the function of accelerating the SNMP GetBulk operation.

Example

Enable the function of accelerating the SNMP GetBulk operation.

```
<Huawei> system-view
[Huawei] snmp-agent bulk-fast enable
```

21.1.17 snmp-agent community

Function

The **snmp-agent community** command configures the SNMPv1 or SNMPv2c read-write community name.

The **undo snmp-agent community** command is used to delete the configuration of the community name.

By default, the community name is not configured.

Format

snmp-agent community { **read** | **write** } *community-name* [**mib-view** *view-name* | **acl** *acl-number*] *

undo snmp-agent community *community-name*

Parameters

Parameter	Description	Value
read	Indicates that the community with a specified name has the read-only rights in the specified view.	-
write	Indicates that the community with a specified name has the read-write rights in the specified view.	-
community-name	Specifies the name of a community. The community name is displayed in cipher text in the configuration file.	The value is a string of 6 to 32 characters or 88 characters case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string. ● When the community name is a string of 6 to 32 characters, the string is processed as plain text by default and will be encrypted. ● When the community name is a string of 88 characters, the string is processed as cipher text by default, and the system will determine whether the string can be parsed. By default, the complexity check is enabled for a community name. If a community name fails the complexity check, the community name cannot be configured. **NOTE** The device has the following requirements for community name complexity: ● The default minimum length of a community name is six characters. ● A community name includes at least two kinds of characters, which can be uppercase letters, lowercase letters, digits, and special characters.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mib-view *view-name*	Specifies a MIB view that the community name can access. • If no MIB view that the community name can access is specified, the community name can access only the default MIB view, that is, ViewDefault. • If a MIB view that the community name can access is specified, the community name can access the specified MIB view.	It is a string of 1 to 32 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
acl *acl-number*	Specifies the ACL corresponding to the community name. **NOTE** Currently, SNMP supports only basic ACLs.	The value is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When running the **snmp-agent community** command, you can select parameters based on the networking requirements.

- To grant the NMS read-only permission in the specified view, configure **read**.
- To grant the NMS read-write permission in the specified view, configure **write**.
- To allow specified NMSs using this community name have the rights of ViewDefault, omit **mib-view** *view-name*.
- To allow all NMSs using this community name to manage specified objects on a managed device, omit **acl** *acl-number*.
- To allow specified NMSs using this community name to manage specified objects on a managed device, configure **mib-view** and **acl**.

Copyright © Huawei Technologies Co., Ltd.

NOTE

When both community name and ACL are configured, the NMS verifies the community name before accessing the device, and then checks the ACL rules. If the community name does not exist, the packet is discarded and a log indicating that the community name is wrong is printed. The ACL rule is not checked. That is, the ACL rule is checked only when the community name exists.

You can run the **display snmp-agent community** command to view the current community name.

Precautions

When you configure a community name in cipher text that starts and ends with %@%@ (the community name can be decrypted by the device), the community name is displayed in the same manner as the configured one in the configuration file. Do not use this setting.

If you specify the parameter **mib-view** or **acl** when running the **snmp-agent community** command, configure the MIB view and ACL rule. If the default MIB view is deleted, the NMS using this community name cannot communicate with managed devices. To continue to use this community name, specify an existing MIB view.

Example

Set the name of a community to **comaccess1** and configure the read-only rights for the community.

```
<Huawei> system-view
[Huawei] snmp-agent community read comaccess1
```

Set the name of a community to **comaccess2** and configure the read-write rights for the community.

```
<Huawei> system-view
[Huawei] snmp-agent community write comaccess2
```

Related Topics

21.1.1 display snmp-agent community

21.1.18 snmp-agent complexity-check disable

Function

The **snmp-agent complexity-check disable** command disables complexity check for community names and SNMPv3 authentication and encryption passwords.

The **undo snmp-agent complexity-check disable** command enables complexity check for community names and SNMPv3 authentication and encryption passwords.

By default, complexity check for community names and SNMPv3 authentication and encryption passwords is enabled.

Copyright © Huawei Technologies Co., Ltd.

Format

snmp-agent complexity-check disable

undo snmp-agent complexity-check disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To improve maintenance efficiency in secure environment, disable complexity check for community names and SNMPv3 passwords by running the **snmp-agent complexity-check disable** command. After complexity check is disabled, the minimum length of a community name or SNMPv3 password is 1, and the community name or password must contain at least one type of characters.

If a community name or SNMPv3 password does not meet complexity requirements, the system is prone to attacks from malicious users, affecting system security. Therefore, you are advised to run the **undo snmp-agent complexity-check disable** command to enable complexity check for community names and SNMPv3 passwords. After complexity check is enabled, the community names or SNMPv3 authentication and encryption passwords must meet the following requirements:

- A community name contains at least six characters. An SNMPv3 authentication or encryption password contains at least eight characters.
- A community name or password must be a combination of at least two of the following: uppercase letters, lowercase letters, digits, and special characters (excluding spaces).
- An SNMPv3 authentication password cannot be the same as an SNMPv3 encryption password.

Example

Disable complexity check for community names or SNMPv3 authentication and encryption passwords.

```
<Huawei> system-view
[Huawei] snmp-agent complexity-check disable
```

Related Topics

21.1.17 snmp-agent community

 Copyright © Huawei Technologies Co., Ltd.

21.1.19 snmp-agent community simple

Function

The **snmp-agent community simple** command enables plain text mode for the community names of SNMPv1 and SNMPv2c.

The **undo snmp-agent community simple** command disables plain text mode for the community names.

By default, community names are not transmitted in plain text.

Format

snmp-agent community simple { **read** | **write** } *community-name* [**mib-view** *view-name* | **acl** *acl-number*] *

undo snmp-agent community simple

Parameters

Parameter	Description	Value
read	Indicates that a community name has the read permission in the specified MIB view.	-
write	Indicates that a community name has the read and write permission in the specified MIB view.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
community-name	Specifies a community name, which is displayed in plain text in the configuration file.	The value is a string of 6 to 32 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces. **NOTE** The community name must meet the following requirements: • The community name contains at least six characters. • The community name must be a combination of at least two of the following: uppercase letters, lowercase letters, digits, and special characters. • By default, the system checks the community name complexity. The community name that fails the check is not allowed.
mib-view *view-name*	Specifies the MIB view that a community name can access. • If no MIB view is specified for a community name, this community name can access only the default MIB view, ViewDefault. • If a MIB view is specified for a community name, this community name can access only the specified MIB view.	The value is a string of 1 to 32 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
acl *acl-number*	Specifies the ACL number matching the community name. **NOTE** SNMP supports only the basic ACL, but does not support advanced or MPLS-based ACL. The specified ACL takes effect for both IPv4 and IPv6 networks.	The value is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When running the **snmp-agent community simple** command to enable plain text mode for SNMPv1 and SNMPv2c read-write community names, select the parameters as required:

- To grant only the read right to the NMS in the specified view (for example, for an administrator with a low level), use the **read** parameter.
- To grant the read and write rights to the NMS in the specified view (for example, for an administrator with a high level), use the **write** parameter.
- To allow some NMSs using a community name to access the MIB view Viewdefault, do not specify the **mib-view** *view-name* parameter.
- To allow some NMSs using a community name to manage certain objects, specify both **mib-view** and **acl**.

NOTE

When both community name and ACL are configured, the NMS checks the community name and then the ACL before accessing the device. If a community name does not exist, packets are discarded and the system prints a community name error log. In addition, the system does not check ACL. That is, the system checks ACL only when the community name exists.

To view the current community name, run the **display snmp-agent community** command.

Precautions

If the **mib-view** or **acl** parameter is specified in the **snmp-agent community** command, configure the MIB view and ACL rules. Do not delete the default MIB view. If it is deleted, the NMS and managed device using this community name cannot set up a connection. To use this community name again, specify an existing MIB view.

Example

Enable plain text mode for the community name **comaccess1** and grant only the read right to the community name.

```
<Huawei> system-view
[Huawei] snmp-agent community simple read comaccess1
```

Enable plain text mode for the community name **comaccess2** and grant the read and write rights to the community name.

```
<Huawei> system-view
[Huawei] snmp-agent community simple write comaccess2
```

Related Topics

21.1.1 display snmp-agent community

 Copyright © Huawei Technologies Co., Ltd.

21.1.20 snmp-agent extend error-code enable

Function

The **snmp-agent extend error-code enable** command enables the function of sending extended error codes to the NMS on the device.

The **undo snmp-agent extend error-code enable** command disables the function of sending extended error codes to the NMS.

By default, the function of sending extended error codes to the NMS is disabled.

Format

snmp-agent extend error-code enable

undo snmp-agent extend error-code enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If the NMS and managed device are Huawei devices, error codes are extended and more scenarios are defined after the function of sending extended error codes is enabled. As a result, users are enabled to locate and troubleshoot faults quickly and accurately.

Support of the MIB for the extended error code:

- For the MIB that supports the extended error code, you can enable the SNMP extended error code function and use Huawei NMS to provide the NMS with various error codes.
- For the MIB that does not support the extended error code, after the SNMP extended error code function is enabled, NMS of either Huawei or other vendors can obtain only the standard error code.

Example

Enable the function of sending extended error codes to the NMS on the device.

```
<Huawei> system-view
[Huawei] snmp-agent extend error-code enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.2 display snmp-agent extend error-code status

21.1.21 snmp-agent group

Function

The **snmp-agent group** command creates an SNMP group by mapping SNMP users to SNMP views.

The **undo snmp-agent group** command deletes a specified SNMP user group.

By default, no SNMP group is configured.

Format

snmp-agent group v3 *group-name* { **authentication** | **noauth** | **privacy** } [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view* | **acl** *acl-number*] *

undo snmp-agent group v3 *group-name* { **authentication** | **noauth** | **privacy** }

Parameters

Parameter	Description	Value
v3	Indicates that the SNMP group uses the security mode in SNMPv3.	-
group-name	Specifies the name of an SNMP group.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
authentication | **noauth** | **privacy**	Indicates the security level of the SNMP group. • **authentication**: indicates that SNMP messages are authenticated but not encrypted. • **noauth**: indicates that SNMP messages are neither authenticated nor encrypted. • **privacy**: indicates that SNMP messages are authenticated and encrypted.	For security purposes, it is recommended that you set the security level of the SNMP group to **privacy**.
read-view *read-view*	Specifies a read-only view.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. *read-view* specified by the **snmp-agent mib-view** command.
write-view *write-view*	Specifies a read-write view.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. *write-view* is specified by the **snmp-agent mib-view** command.
notify-view *notify-view*	Specifies a notify view.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. *notify-view* is specified by the **snmp-agent mib-view** command.
acl *acl-number*	Specifies a basic ACL.	The value is an integer that ranges from 2000 to 2999.

Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SNMPv1 and SNMPv2c have serious defects in terms of security. The security authentication mechanism used by SNMPv1 and SNMPv2c is based on the community name. In this mechanism, the community name is transmitted in plain text. You are not advised to use SNMPv1 and SNMPv2c on untrusted networks.

By adopting the user-based security model, SNMPv3 eradicates the security defects in SNMPv1 and SNMPv2c and provides two services, authentication and privacy. The SNMP group name and security name determine an SNMP group. SNMPv3 defines the following security levels:

- noAuthNoPriv
- AuthNoPriv
- AuthPriv

NOTE

The security authentication level noAuthPriv does not exist. This is because the generation of a key is based on the authentication information and product information.

The **snmp-agent group** command can be used to configure the following:

- Authentication
- Privacy
- Access rights for users of SNMP group
- Bind the SNMP group to a MIB view

Parameters are selected based on the following rules:

- To enhance security, configure the parameter **authentication** or **privacy**.
  - If neither **authentication** nor **privacy** are configured, SNMP messages are not authenticated or encrypted. This applies to the environment that is secure and has a fixed administrator.
  - To authenticate SNMP messages without encryption, configure the parameter **authentication**. This mode is applicable to secure networks managed by many administrators who may frequently perform operations on the same device. Authentication allows only the administrators with permission to access the device.
  - To authenticate and encrypt SNMP messages, configure the parameter **privacy**. This mode is applicable to insecure networks managed by many administrators who may frequently perform operations on the same device. Authentication and encryption allow only specified administrators to access the device and encrypts data before the transmission. This prevents data from being tampered or leaked.

Copyright © Huawei Technologies Co., Ltd.

- To grant the NMS read-only permission in the specified view, configure **read-view**. To grant the NMS read-write permission in the specified view, configure **write-view**.

  To filter unnecessary alarms, configure **notify-view**. After this parameter is configured, only alarms generated on MIB objects specified by **notify-view** are delivered to the NMS.

  By default, the read-only view of an SNMP group is the ViewDefault view, and the names of the read-write view and inform view are not specified.
- To allow specified NMSs in the same SNMPv3 group to access the device, configure **acl**.

Configuration Impact

When you run the **undo snmp-agent group** command to delete an SNMP user group, you delete all SNMP users in the SNMP user group.

Precautions

To receive trap messages specified in *notify-view*, you need to ensure the target host for receiving SNMP traps is specified through the **snmp-agent target-host trap-hostname** command.

User access can be encrypted and authenticated, authenticated but not encrypted, or neither authenticated nor encrypted. If the access level of a user is lower than the security level of the specified group, the access fails. When the groups that a user can access have multiple security levels, the user can select the group with the highest security level among the groups that can be accessed, and access the view of the group.

Example

Create an SNMPv3 group named **Johngroup**, authenticate and encrypt SNMP messages, and configure the view that the SNMPv3 group can read only to public.

```
<Huawei> system-view
[Huawei] snmp-agent
[Huawei] snmp-agent mib-view excluded public 1.3.6.1.2.1
[Huawei] snmp-agent group v3 Johngroup privacy read-view public
```

Create an SNMPv3 group named **Johngroup**, authenticate and encrypt SNMP messages, and configure the view that the SNMPv3 group write-view to private.

```
<Huawei> system-view
[Huawei] snmp-agent
[Huawei] snmp-agent mib-view included private 1.3.6.1.2.1
[Huawei] snmp-agent group v3 Johngroup privacy write-view private
```

Related Topics

21.1.23 snmp-agent mib-view

21.1.37 snmp-agent usm-user

21.1.3 display snmp-agent group

Copyright © Huawei Technologies Co., Ltd.

21.1.22 snmp-agent local-engineid

Function

The **snmp-agent local-engineid** command sets an engine ID for the local SNMP agent.

The **undo snmp-agent local-engineid** command restores the engine ID of the local SNMP agent to the default value.

By default, the device uses an internal algorithm to automatically generate an engine ID for a device. The engine ID consists of the enterprise number and the device information.

Format

snmp-agent local-engineid { *engineid* | **sysname** }

undo snmp-agent local-engineid

Parameters

Parameter	Description	Value
engineid	Specifies the engine ID of the local SNMP agent.	The value is string of 10 to 64 hexadecimal digits.
sysname	Indicates the engine ID generated based on the system name.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **snmp-agent local-engineid** command to set an engine ID for the local SNMP agent for identification.

The SNMP engine ID uniquely identifies an SNMP agent in a management domain. The SNMP engine ID is an important component of the SNMP agent. It schedules and processes SNMP messages, and implements security authentication and access control. You can use the **display snmp-agent local-engineid** command to check the engine ID of the local SNMP entity.

When setting an engine ID, you need to comply with the following rules:

- The length of the octet strings varies. The first four octets are set to the binary equivalent of the agent, which is SNMP management private

Copyright © Huawei Technologies Co., Ltd.

enterprise number and is assigned by the Internet Assigned Numbers Authority (IANA). The engine ID of Huawei devices is 2011 in decimal notation. The first digit is in binary format, and has a fixed value 1. Therefore, the engine ID in hexadecimal format is 800007DB.

- The device information can be configured manually. It is recommended that the IP address or MAC address of the device be used as the device information to uniquely identify the device.

Precautions

If the local engine ID is set or changed, the existing SNMPv3 user with this engine ID is deleted. If the original engine ID is restored, the corresponding user configuration is restored.

After the SNMP agent function is enabled using the **snmp-agent** command, the system automatically adopts the default engine ID for the local SNMP agent.

The password summary used by SNMPv3 users is calculated using MD5 or SHA based on the user password and engine ID of the local SNMP agent. If the engine ID of the local SNMP agent is changed, the generated password summary becomes invalid. As a result, a new password summary needs to be generated for SNMPv3 users.

Example

Set the engine ID of the local SNMP agent to 800007DB03360102101100.

```
<Huawei> system-view
[Huawei] snmp-agent local-engineid 800007DB03360102101100
Info: Modify the local-engineid will disable the configured SNMPv3 user, all
users must be reconfigured, proceed? (y/n)[n]:y
```

Related Topics

21.1.4 display snmp-agent local-engineid

21.1.37 snmp-agent usm-user

21.1.23 snmp-agent mib-view

Function

The **snmp-agent mib-view** command creates or updates a MIB view.

The **undo snmp-agent mib-view** command cancels the configuration of the current MIB view.

By default, the MIB view name is ViewDefault, and the MIB subtree includes lagMIB nodes and all internet subnodes except for snmpVacmMIB and snmpUsmMIB.

Format

snmp-agent mib-view *view-name* { **exclude** | **include** } *subtree-name* [**mask** *mask*]

undo snmp-agent mib-view *view-name* [*subtree-name*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
view-name	Specifies the MIB view name.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
exclude	Excludes the MIB subtree.	-
include	Includes the MIB subtree.	-
subtree-name	Specifies the name of the subtree, which identifies a subtree uniquely. *subtree-name* can be the OID (such as 1.4.5.3.1) or the name (such as system) of the subtree.	It is a string of 1 to 128 characters, which are case sensitive and cannot be blank spaces. **NOTE** It must be a valid MIB subtree.
mask	Indicates the subtree mask, which specifies the access range of the view.	-
mask	Specifies the value of the subtree mask. This parameter specifies the mode and length of the matching between the user operation node and the subtree included by the view.	The value is a hexadecimal string of 1 to 32 characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A MIB view is an abstract set of all managed objects. The NMS manages the device by reading and writing the managed objects in the MIB. A MIB view defines management information included and excluded in this MIB view.

If you forget which information you have configured for a MIB view, you can run the **display snmp-agent mib-view** command to check it.

Precautions

If both the **include** and **exclude** parameters are configured for MIB objects that have an inclusion relationship, whether to include or exclude the lowest MIB

Copyright © Huawei Technologies Co., Ltd.

object will be determined by the parameter configured for the lowest MIB object. For example, the snmpV2, snmpModules, and snmpUsmMIB objects are from top down in the MIB table. If the **exclude** parameter is configured for snmpUsmMIB objects and **include** is configured for snmpV2, snmpUsmMIB objects will still be excluded.

When using the **snmp-agent mib-view** command, note the following:

- A view name uniquely identifies a view. Configuring the same view name repeatedly is equivalent to adding the subtree to the view. The system displays prompt information when a subtree is overwritten due to the repeated subtree configuration. The default view cannot be deleted.
- The system checks the subtree name. The configured subtree must be the one existing in the MIB tree. The subtree name is configurable.
- The rule of smallest range is adopted for the access rights of the leaf node. That is, the MIB subtree configured with the include/exclude rights at the most internal layer determines the authority of the leaves inside the subtree.
- Only an existing view can be deleted regardless of whether the view is referenced or not.
- The total number of subtrees in all views cannot exceed 20.
- A leaf node of the MIB tree defines the managed object of the device, such as the routing table. The leaf node with a unique value is called a scalar, and the leaf node with multiple values is called a variable.
- To set the security level to privacy or authentication, you must run the **snmp-agent mib-view** *view-name* **include** *subtree-name* command to configure the MIB view information and the included MIB subtree.

An input mask must meet the following requirements:

- The mask is a hexadecimal string.
- The bit converted to 1 (a binary number) indicates that the subtree matches the corresponding sub IDs exactly. The bit converted to 0 (a binary number) indicates that the subtree matches the sub IDs universally.
- After the mask is converted to a binary string, the length of the string should not less than the number of the sub IDs of the subtree. In addition, 0 must exist before 1.
- A view record without a mask indicates that the view matches the subtrees completely.

Example

Configure MIB view **a1** that includes the internet subtree.

```
<Huawei> system-view
[Huawei] snmp-agent mib-view a1 include internet
```

Related Topics

21.1.5 display snmp-agent mib-view

21.1.17 snmp-agent community

21.1.21 snmp-agent group

Copyright © Huawei Technologies Co., Ltd.

21.1.24 snmp-agent notify-filter-profile

Function

The **snmp-agent notify-filter-profile** command creates or updates a trap filter profile.

The **undo snmp-agent notify-filter-profile** command deletes a trap filter profile.

By default, no trap is filtered.

Format

snmp-agent notify-filter-profile { **include** | **exclude** } *profile-name oid-tree*

undo snmp-agent notify-filter-profile *profile-name* [*oid-tree*]

Parameters

Parameter	Description	Value
include	Includes the specified MIB subtree. **NOTE** The **include** parameter is configured to filter traps of a certain type that are sent to the destination host. In addition to configuring the trap object, you need to configure all the objects of the parameter bound to the trap object.	-
exclude	Excludes the specified MIB subtree. **NOTE** The **exclude** parameter is configured to filter traps of a certain type that are not sent to the destination host.	-
profile-name	Specifies the name of a trap filter profile.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
oid-tree	Specifies the OID for the MIB subtree. *oid-tree* can be the OID (such as 1.4.5.3.1) or the name (such as system) of the subtree.	The value is a string of 1 to 128 case-sensitive characters without spaces. **NOTE** It must be a valid MIB subtree.

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

To filter the traps sent to a destination host, run the **snmp-agent notify-filter-profile** command to configure a trap filter profile and specify the MIB object to be filtered in the profile.

Before sending a trap message to a target host, the device checks whether the alarm object and parameter binding object are within the filtering range of the target host. If this trap is within the filtering range, the device does not send the trap message; otherwise, the device sends the trap message.

NOTE

If no trap filter profile is configured, all traps are sent to the destination host.

Example

Configure a trap filter profile named **tmp**.

```
<Huawei> system-view
[Huawei] snmp-agent notify-filter-profile include tmp linkDown
```

Related Topics

21.1.6 display snmp-agent notify-filter-profile

21.1.25 snmp-agent permit interface

Function

The **snmp-agent permit interface** command specifies physical interfaces on the device to which the NMS can connect.

The **undo snmp-agent permit interface** command restores the default physical interfaces on the device to which the NMS can connect.

By default, the NMS can connect to all the physical interfaces on the device.

Format

snmp-agent permit interface { *interface-type interface-number* } &<1-5>

undo snmp-agent permit interface

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	*interface-type*: specifies the interface type. *interface-number*: specifies the interface number. *interface-number* and *interface-type* specify an interface.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent the NMS from connecting to the device through an unauthorized physical interface, you can run the **snmp-agent permit interface** command to specify physical interfaces on the device to which the NMS can connect.

Precautions

- By default, the NMS can connect to all the physical interfaces on the device. When you run this command to specify one physical interface on the device, the NMS cannot connect to the other physical interfaces on the device.
- You can specify a maximum of five interfaces each time you run the **snmp-agent permit interface** command. The latest configuration overrides the previous one. For example, before you run the command, the NMS can connect to three physical interfaces GigabitEthernet 1/0/0, GigabitEthernet 2/0/0, and GigabitEthernet 3/0/0 on the device. After you run the command to specify the interface GigabitEthernet 1/0/0, the NMS can only connect to the interface GigabitEthernet 1/0/0.

Example

Specify physical interfaces on the device to which the NMS can connect.

```
<Huawei> system-view
[Huawei] snmp-agent permit interface gigabitethernet 1/0/0 gigabitethernet 2/0/0
  Info: Succeeded in setting snmp permit interface.
```

Restore the default physical interfaces on the device to which the NMS can connect.

```
<Huawei> system-view
[Huawei] undo snmp-agent permit interface
```

 Copyright © Huawei Technologies Co., Ltd.

21.1.26 snmp-agent sys-info

Function

The **snmp-agent sys-info** command sets the SNMP system information.

The **undo snmp-agent sys-info** command restores the default setting.

By default, the system maintenance information is " R&D Shenzhen, Huawei Technologies Co.,Ltd.": the system location is Shenzhen China" and the version is SNMPv3.

Format

snmp-agent sys-info { **contact** *contact* | **location** *location* | **version** { { **v1** | **v2c** | **v3** } * | **all** } }

undo snmp-agent sys-info { **contact** | **location** | **version** { { **v1** | **v2c** | **v3** } * | **all** } }

Parameters

Parameter	Description	Value
contact *contact*	Indicates contact information of system maintenance.	The value is a string of 1 to 225 case-sensitive characters that can contain spaces.
location *location*	Indicates the location of a device.	The value is a string of 1 to 255 case-sensitive characters that can contain spaces.
version { { **v1** | **v2c** | **v3** } * | **all** }	Indicates the SNMP version. • **v1**: SNMPv1 is enabled. • **v2c**: SNMPv2c is enabled. • **v3**: SNMPv3 is enabled. • **all**: SNMPv1, SNMPv2c, and SNMPv3 are enabled.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

To configure the contact information for the managed node, you can run the **snmp-agent sys-info contact** command in the system. If a device fails, maintenance personnel can contact the vendor for device maintenance.

To configure the physical location of the node, you can run the **snmp-agent sys-info location** command in the system.

To configure features in a specified version, you can run the **snmp-agent sys-info version** command to set the corresponding SNMP version in the system. SNMPv1 or SNMPv2c is not secure enough. Using SNMPv3 is recommended.

SNMPv1:

- Community-name-based access control
- MIB-view-based access control

SNMPv2c:

- Community-name-based access control
- MIB-view-based access control

Besides inheriting basic SNMPv2c operations, SNMPv3 defines a management architecture, which introduces a User-based Security Model (USM) to provide users with a more secure access mechanism.

- User group
- Group-based access control
- User-based access control
- Authentication and encryption mechanisms

NOTE

Use **display snmp-agent sys-info** command to view the information of the system maintenance, the physical location of the node and the SNMP version.

Precautions

A lack of authentication capabilities in SNMPv1 and SNMPv2c results in vulnerability to security threats, so SNMPv3 is recommended.

Example

Set the contact information of the system maintenance as "call Operator at 010-12345678".

```
<Huawei> system-view
[Huawei] snmp-agent sys-info contact call Operator at 010-12345678
```

Set the location of a device as "shanghai China".

```
<Huawei> system-view
[Huawei] snmp-agent sys-info location shanghai China
```

Set the current SNMP version used by the system to SNMPv2c.

```
<Huawei> system-view
[Huawei] snmp-agent sys-info version v2c
```

Related Topics

21.1.8 display snmp-agent sys-info

 Copyright © Huawei Technologies Co., Ltd.

21.1.27 snmp-agent target-host trap-hostname

Function

The **snmp-agent target-host trap-hostname** configures the target host of trap messages.

The **undo snmp-agent target-host trap-hostname** deletes the target host of trap messages.

By default, no target host of trap messages is configured.

Format

snmp-agent target-host trap-hostname *hostname* **address** { *ipv4-addr* [**udp-port** *udp-portid*] [**public-net** | **vpn-instance** *vpn-instance-name*] | **ipv6** *ipv6-addr* [**udp-port** *udp-portid*] } **trap-paramsname** *paramsname* [**notify-filter-profile** *profile-name*]

undo snmp-agent target-host trap-hostname *hostname*

Parameters

Parameter	Description	Value
hostname	Specifies the name of the target host.	The name a string of 1 to 32 case-sensitive characters without spaces.
address *ipv4-addr*	Indicates the IP address of the target host.	The value is in dotted decimal notation.
udp-port *udp-portid*	Indicates the ID of the port on the target host for receiving trap messages.	The value is an integer that ranges from 1 to 65535. The default value is 162.
public-net	Indicates that the target host connects the alarm host on the public network.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Indicates the name of a VPN instance.	The name a string of 1 to 31 case-sensitive characters without spaces.
ipv6-address *ipv6-address*	Specifies the IPv6 address of the target host.	The value is a hexadecimal number that ranges from 0 to FFFF (0::0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff, "::" indicates that the value of the field between the two colons is 0).
udp-port *udp-portid*	Indicates that the target host receives port numbers of trap messages.	The value is an integer that ranges from 1 to 65535.
trap-paramsname *paramsname*	Indicates the name of the trap sending parameter list used by the target host.	The name a string of 1 to 32 case-sensitive characters without spaces.
notify-filter-profile *profile-name*	Specifies the name of a trap filter profile.	The name a string of 1 to 32 case-sensitive characters without spaces.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Only the terminal configured as the target host of trap messages can receive traps. The NMS is generally configured as the target host of trap messages. Currently, the system supports a maximum of 20 target hosts.

Example

Set the IP address of the target host to 10.1.1.1, the host name to aaa, and the trap sending parameter list name to abc.

```
<Huawei> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei] snmp-agent target-host trap-hostname aaa address 10.1.1.1 trap-paramsnam abc
```

21.1.28 snmp-agent target-host trap-paramsname

Function

The **snmp-agent target-host trap-paramsname** command configures parameters for sending trap messages. The trap sending parameter list is composed of these parameters.

The **undo snmp-agent target-host trap-paramsname** command deletes a trap sending parameter list.

Format

snmp-agent target-host trap-paramsname *paramsname* { { **v1** | **v2c** } **securityname** *securityname* | **v3 securityname** *securityname* { **authentication** | **noauthnopriv** | **privacy** } } [**binding-private-value**] [**private-netmanager**]

undo snmp-agent target-host trap-paramsname *paramsname*

Parameters

Parameter	Description	Value
paramsname	Specifies the name of a trap sending parameter list.	The value is a string of 1 to 32 characters.
v1	Indicates SNMPv1. This parameter specifies SNMPv1 as the trap message sending protocol.	-
v2c	Indicates SNMPv2c. This parameter specifies SNMPv2c as the trap message sending protocol.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
v3	Indicates SNMPv3. SNMPv3 protocol contains the basic functions of SNMPv1 and SNMPv2 and defines a series of management functions for network security and access control. This parameter specifies SNMPv3 as the trap message sending protocol.	-
securityname *securityname*	Indicates the host name in the trap message. When the trap sending protocol is the SNMPv3 protocol, this parameter is the user name in the SNMPv3 group.	The value is a string. The string length range is • 1 to 32 characters in plain text. • 48 to 68 characters in cipher text.
authentication	Authenticates but not encrypts trap messages. When the trap sending protocol is SNMPv3, this parameter can authenticate (the receiver) but not encrypt (the sender) trap messages.	-
noauthnopriv	Authenticates and encrypts no trap message. When the trap sending protocol is SNMPv3, this parameter is used as if no trap message needs to be authenticated (the receiver) or encrypted (the sender).	-
privacy	Authenticates and encrypts trap messages. When the trap sending protocol is SNMPv3, this parameter can authenticate (the receiver) and encrypt (the sender) trap messages.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
binding-private-value	Indicates that trap messages sent to a target host carry extended bound variables. If alarm objects defined in public MIBs are extended on a Huawei data communication device, you can use the **binding-private-value** parameter to determine whether the corresponding trap messages sent from the device to an NMS carry extended bound variables. • If the **binding-private-value** parameter is not specified, the trap message does not carry extended bound variables. The **binding-private-value** parameter is not recommended when the NMS is a third-party NMS. This ensures that the third-party NMS can receive trap messages from Huawei data communication devices. By default, a trap message sent from a Huawei data communication device does not carry extended bound variables. • If the **binding-private-value** parameter is specified, the trap message carries extended bound variables. The **binding-private-value** parameter is recommended when the NMS is a Huawei NMS. This allows more abundant information in trap messages.	-
private-netmanager	# Configure the Huawei NMS as the target host to receive trap messages. After the Huawei NMS is used, the alarm message sent to the Huawei NMS can contain more detailed information, such as the alarm type, alarm ID, and send time of the alarm message.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Currently, the system supports a maximum of 20 trap sending parameter lists.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the trap sending parameter list: set the list name to aaa, set SNMPv3 as the trap sending protocol, set the host name in the SNMP trap as bbb, and authenticate but do not encrypt the trap messages.

```
<Huawei> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei] snmp-agent target-host trap-paramsname aaa v3 securityname bbb authentication
```

Related Topics

21.1.9 display snmp-agent target-host

21.1.27 snmp-agent target-host trap-hostname

21.1.29 snmp-agent trap disable

Function

The **snmp-agent trap disable** command disables the trap function for all features.

The **undo snmp-agent trap disable** command restores the trap function for all features to the default status.

By default, the **display snmp-agent trap all** command can be used to view the status of the trap function for all features.

Format

snmp-agent trap disable

undo snmp-agent trap disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the trap function for all modules, run the **snmp-agent trap enable** command. To enable the trap function for a specified module, run the **snmp-agent trap enable feature-name** command.

- To disable the trap function for all modules, run the **snmp-agent trap disable** command.
- To restore the trap function for all features to the default status, run the **undo snmp-agent trap disable** or **undo snmp-agent trap enable** command.

Copyright © Huawei Technologies Co., Ltd.

NOTE

To disable the trap function for a specified module, run the **undo snmp-agent trap enable feature-name** command.

Example

Disable the trap function for all features.

```
<Huawei> system-view
[Huawei] snmp-agent trap disable
```

Related Topics

21.1.10 display snmp-agent trap all

21.1.30 snmp-agent trap enable

Function

The **snmp-agent trap enable** command enables the router to send traps.

The **undo snmp-agent trap enable** command restores the default setting.

The default configuration of the **snmp-agent trap enable** command can be checked by the **display snmp-agent trap all** command.

Format

snmp-agent trap enable

undo snmp-agent trap enable

Parameters

None.

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the trap function for all modules, run the **snmp-agent trap enable** command.

Example

Enable the router to send traps.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.10 display snmp-agent trap all

21.1.31 snmp-agent trap enable feature-name

Function

The **snmp-agent trap enable feature-name** command enables a specified trap for a specified feature.

The **undo snmp-agent trap enable feature-name** command disables a specified trap for a specified feature.

The default configuration of the **snmp-agent trap enable feature-name** command can be checked using the **display snmp-agent trap all** command.

Format

snmp-agent trap enable feature-name *feature-name* [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name *feature-name* [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
feature-name	Specifies the name of the feature that generates traps.	-
trap-name *trap-name*	Specifies the name of a trap.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

If **trap-name** *trap-name* is not specified, the router enables all traps about a specified feature after the **snmp-agent trap enable feature-name** *feature-name* command is used.

You can run the **display snmp-agent trap all** command to check the configuration result.

Example

Enable the router to send the vrrptrapauthfailure trap about VRRP to the NMS.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name vrrp trap-name vrrptrapauthfailure
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.10 display snmp-agent trap all

21.1.32 snmp-agent trap enable feature-name snmp

Function

The **snmp-agent trap enable feature-name snmp** command enables an SNMP trap.

The **undo snmp-agent trap enable feature-name snmp** command disables an SNMP trap.

By default, the coldStart and warmStart traps are enabled and the authenticationFailure trap is disabled.

Format

snmp-agent trap enable feature-name snmp [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name snmp [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
trap-name *trap-name*	Specifies the name of a trap.	The traps are as follows: • authenticationFailure • coldstart • warmstart

Views

System view

Default Level

3: Management level

Usage Guidelines

The **snmp-agent trap enable feature-name snmp** command is used to enable an SNMP trap. After that, the trap generated during the device running will be sent to the NMS. At present, the following SNMP traps are supported:

- coldStart: This trap is generated when the device is powered off and restarted.
- warmStart: This trap is generated when the status of SNMP agent is changed from disable to enable.
- authenticationFailure: This trap is generated when a user uses an incorrect community name and is unable to log in to the device.

Copyright © Huawei Technologies Co., Ltd.

You can run the **display snmp-agent trap feature-name snmp all** command to check the configuration result.

Example

Enable the SNMP authenticationFailure trap.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name snmp trap-name authenticationFailure
```

Related Topics

21.1.11 display snmp-agent trap feature-name snmp all

21.1.33 snmp-agent trap enable syslog

Function

The **snmp-agent trap enable syslog** command enables the function of converting logs to trap messages when syslog is triggered.

The **undo snmp-agent trap enable syslog** command disables the function of converting logs to trap messages when syslog is triggered.

By default, the function of converting logs to trap messages is disabled when syslog is triggered.

Format

snmp-agent trap enable syslog

undo snmp-agent trap enable syslog

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable the function of converting logs to trap messages when syslog is triggered, run the **snmp-agent trap enable syslog** command.

Precautions

To make the command take effect, you need to run the **snmp-agent trap enable** command to enable the router to send trap packets.

Copyright © Huawei Technologies Co., Ltd.

Example

Enable the function of converting logs to trap messages when syslog is triggered.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable syslog
```

Related Topics

21.1.30 snmp-agent trap enable

21.1.34 snmp-agent trap life

Function

The **snmp-agent trap life** command sets the lifetime of trap messages. When the lifetime expires, the trap messages are discarded.

The **undo snmp-agent trap life** command cancels the current settings.

By default, the lifetime of trap messages is 120 seconds.

Format

snmp-agent trap life *seconds*

undo snmp-agent trap life

Parameters

Parameter	Description	Value
seconds	Specifies the lifetime of trap messages.	The value is an integer that ranges from 1 to 2592000, in seconds. The default value is 120.

Views

System view

Default Level

3: Management level

Usage Guidelines

When the lifetime expires, the trap messages are discarded.

Example

Set the lifetime of trap messages to 60 seconds.

```
<Huawei> system-view
[Huawei] snmp-agent trap life 60
```


Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.30 snmp-agent trap enable

21.1.35 snmp-agent trap queue-size

Function

The **snmp-agent trap queue-size** command sets the queue length of the trap messages sent to a target host.

The **undo snmp-agent trap queue-size** command cancels the current settings.

The default value is 100.

Format

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

Parameters

Parameter	Description	Value
size	Specifies the queue length of trap messages.	The value is an integer that ranges from 1 to 1000. The default value is 100.

Views

System view

Default Level

3: Management level

Usage Guidelines

When a large number of trap messages need to be sent in a certain period of time, packets will be lost if the queue length of trap messages is insufficient. The queue length can be adjusted to reduce the packet loss ratio.

When the lifetime of trap messages is long, the queue length of trap messages needs to be lengthened. If the queue length is not lengthened, packet loss will occur.

Example

Set the queue length of the trap messages sent to the target host to 200.

```
<Huawei> system-view
[Huawei] snmp-agent trap queue-size 200
```


Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.30 snmp-agent trap enable

21.1.34 snmp-agent trap life

21.1.36 snmp-agent trap source

Function

The **snmp-agent trap source** command sets the source interface from which traps are sent.

The **undo snmp-agent trap source** command removes the set source interface configuration.

By default, source interface is not set.

Format

snmp-agent trap source *interface-type interface-number*

undo snmp-agent trap source

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the source interface that sends traps.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **snmp-agent trap source** command to specify the type and number of the interface on the device from which traps are sent. The system specifies the IP address of this interface as the source IP address of traps. In this way, the trap source can be identified on the NMS.

Precautions

The source interface that sends traps must have an IP address; otherwise, the commands will fail to take effect. To ensure device security, it is recommended that you set the source IP address to the local loopback address.

Copyright © Huawei Technologies Co., Ltd.

The source interface in traps on the device must be the same as the source interface specified on the NM station. Otherwise, the NM station cannot receive traps.

Example

Specify the IP address of GE1/0/0 as the source address of traps.

```
<Huawei> system-view
[Huawei] snmp-agent trap source gigabitethernet 1/0/0
```

Related Topics

21.1.30 snmp-agent trap enable

21.1.37 snmp-agent usm-user

Function

The **snmp-agent usm-user** command adds a user to an SNMP user group.

The **undo snmp-agent usm-user** command deletes a user from an SNMP user group.

By default, the SNMP user group has no users added.

Format

snmp-agent usm-user v3 *user-name* [**group** *group-name* | **acl** *acl-number*] *

snmp-agent usm-user v3 *user-name* **authentication-mode** { **md5** | **sha** }

snmp-agent usm-user v3 *user-name* **privacy-mode** { **aes128** | **des56** }

undo snmp-agent usm-user v3 *user-name* [**acl** | **authentication-mode** | **group** | **privacy-mode**]

Parameters

Parameter	Description	Value
v3	Indicates that the SNMP user group uses the SNMPv3 security mode.	-
user-name	Specifies a user name.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
group *group-name*	Specifies the name of the SNMP group that the user belongs to.	The value is a string of 1 to 32 case-sensitive characters without spaces.
authentication-mode	Sets the authentication mode. **NOTE** Authentication is a process in which the SNMP agent (or the NMS) confirms that the message is received from an authorized NMS (or SNMP agent) and the message is not changed during transmission. RFC 2104 defines Keyed-Hashing for Message Authentication Code (HMAC), an effective tool that uses the security hash function and key to generate the message authentication code. This tool is widely used in the Internet. HMAC used in SNMP includes HMAC-MD5-96 and HMAC-SHA-96. The hash function of HMAC-MD5-96 is MD5 that uses 128-bit authKey to generate the key. The hash function of HMAC-SHA-96 is SHA-1 that uses 160-bit authKey to generate the key.	-
md5	Uses the HMAC MD5 algorithm for user authentication. Two communication parties share a private key. The sending party uses this key to create a message authentication code (MAC), and the receiving party uses this key to calculate the MAC. If the calculated MAC matches the MAC created by the sending party, the authentication succeeds.	-
sha	Uses the HMAC SHA algorithm for user authentication. The working principle of the HMAC SHA algorithm is similar to that of the HMAC MD5 algorithm. The only difference lies in the methods for generating the MAC. **NOTE** The calculation speed of the HMAC-MD5-96 algorithm is faster than that of the HMAC-SHA-96 algorithm; the HMAC-SHA-96 algorithm is more secure than the HMAC-MD5-96 algorithm. To ensure high security, please use the HMAC-SHA-96 algorithm.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
privacy-mode	Specifies the authentication with encryption. The system adopts the cipher block chaining (CBC) code of the data encryption standard (DES) and uses 128-bit privKey to generate the key. The NMS uses the key to calculate the CBC code and then adds the CBC code to the message while the SNMP agent fetches the authentication code through the same key and then obtains the actual information. Like the identification authentication, the encryption requires the NMS and the SNMP agent to share the same key to encrypt and decrypt the message.	-
aes128	The 128-bit AES encryption algorithm is used to encrypt the PDU of packets. Each user has a key and uses this key to encrypt data using the AES algorithm and sends the encrypted data together with user information to the receiving party. After receiving the data, the receiving party obtains the key from the user information, and calculates the encrypted data based on the AES algorithm to obtain the plain text.	-
des56	The 56-bit DES encryption algorithm is used to encrypt the PDU of packets. Each user has a key and uses this key to encrypt data using the DES algorithm and sends the encrypted data together with user information to the receiving party. After receiving the data, the receiving party obtains the key from the user information, and calculates the encrypted data based on the DES algorithm to obtain the plain text.	-
acl *acl-number*	Specifies the ACL number.	The value is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

SNMPv1 and SNMPv2c have serious defects in terms of security. The security authentication mechanism used by SNMPv1 and SNMPv2c is based on the community name. In this mechanism, the community name is transmitted in plain text. You are not advised to use SNMPv1 and SNMPv2c on untrusted networks.

By adopting the user-based security model, SNMPv3 eradicates the security defects in SNMPv1 and SNMPv2c and provides two services, authentication and encryption. The user-based security model defines three security authentication levels: noAuthNoPriv, AuthNoPriv, and AuthPriv.

NOTE

The security authentication level noAuthPriv does not exist. This is because the generation of a key is based on the authentication information and product information.

Different from SNMPv1 and SNMPv2c, SNMPv3 can implement access control, identity authentication, and data encryption through the local processing model and user security model. SNMPv3 can provide higher security and confidentiality than SNMPv1 and SNMPv2c. The following table lists the difference between SNMPv1, SNMPv2c, and SNMPv3:

Table 21-14 Comparison in the security of SNMP of different versions

Protocol version	User Checksum	Encryption	Authentication
v1	Adopts the community name.	None	None
v2c	Adopts the community name.	None	None
v3	Adopts user name-based encryption/ decryption.	Yes	Yes

The **snmp-agent group** command can be used to configure the authentication, encryption, and access rights for an SNMP group. The **snmp-agent group** command can be used to configure the rights for users in a specified SNMP group and bind the SNMP group to a MIB view. The MIB view is created through the **snmp-agent mib-view** command. For details, see the usage guideline of this command. After an SNMP user group is configured, the MIB-view-based access control is configured for the SNMP user group. Users cannot access objects in the MIB view through the SNMP user group. The purpose of adding SNMP users to an SNMP user group is to ensure that SNMP users in an SNMP user group have the same security level and access control list. When you run the **snmp-agent usm-user** command to configure a user in an SNMP user group, you configure the MIB-view-based access rights for the user. If an SNMP user group is configured with the AuthPriv access rights, you can configure the authentication mode and encryption mode when configuring SNMP users. Note that the authentication keys

 Copyright © Huawei Technologies Co., Ltd.

and encryption passwords configured on the NMS and the SNMP agent should be the same; otherwise, authentication fails.

When the NMS and device are in an insecure network environment, for example, a network prone to attacks, it is recommended that you configure different authentication password and encryption password to improve security.

Configuration Impact

If an SNMP agent is configured with a remote user, the engine ID is required during the authentication. If the engine ID changes after the remote user is configured, the remote user becomes invalid.

Precautions

The user security level must be higher than or equal to the security level of the SNMP user group to which the user is added.

The security level of an SNMP user group can be (in descending order):

- Level 1: privacy (authentication and encryption)
- Level 2: authentication (without encryption)
- Level 3: none (neither authentication nor encryption)

The user security level must be higher than the user group level. For example, if the security level of an SNMP user group is level 1, the security level of the user that is added to the group must be level 1; if the security level of an SNMP user group is level 2, the security level of the user that is added to the group can be level 1 or level 2.

To add an SNMP user to an SNMP group, ensure that the SNMP user group is valid.

If you run the **snmp-agent usm-user** command multiple times, only the latest configuration takes effect.

Keep your user name and plain-text password well when creating the user. The plain-text password is required when the NMS accesses the device.

Note that MD5 and DES56 encryption algorithm cannot ensure security. SHA and AES128 encryption algorithm is recommended.

Example

Configure an SNMPv3 user with user name **u1**, group name **g1**, authentication mode **SHA**, authentication password **8937561bc**, encryption mode **AES128**, and encryption password **68283asd**

```
<Huawei> system-view
[Huawei] snmp-agent usm-user v3 u1 group g1
[Huawei] snmp-agent usm-user v3 u1 authentication-mode sha
Please configure the authentication password (<8-64>)
Enter Password:
Confirm Password:
[Huawei] snmp-agent usm-user v3 u1 privacy-mode aes128
Please configure the privacy password (<8-64>)
Enter Password:
Confirm Password:
[Huawei]
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.21 snmp-agent group

21.1.38 snmp-agent source loopback

Function

The **snmp-agent source loopback** command configures a Loopback interface as the source interface for sending packets.

The **undo snmp-agent source** command restores the default source interface for sending packets.

By default, the source interface for sending packets is a physical outbound interface.

Format

snmp-agent source loopback *loopback-number*

undo snmp-agent source

Parameters

Parameter	Description	Value
loopback-number	Specifies the number of a Loopback interface.	The value is an integer, and the value range varies depending on the device model.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the NMS sends a get operation request to the device, the device replies with a response packet. The response packet carries source interface information. The device uses the IP address of this interface as the source address of packets. When an ACL is configured on the NMS to filter the packets sent from the device, the ACL rules vary according to source interface IP addresses, and communication may be affected by interface status. After a Loopback interface is configured as the source interface for response packets using the **snmp-agent source loopback** command, the impact of source address difference and interface status can be avoided by specifying the source address in an ACL rule as this Loopback interface address. This configuration allows the device to filter outgoing packets and protect security. In addition, the configurations of ACL rules and security policies are simplified.

Copyright © Huawei Technologies Co., Ltd.

Precautions

Loopback interface that will be configured as the source interface must exist on the device and has an IPv6 address. Otherwise, command execution will fail.

Example

Set Loopback0 as the source interface for sending packets.

```
<Huawei> system-view
[Huawei] snmp-agent source loopback 0
```

21.1.39 snmp-agent server-source

Function

The **snmp-agent server-source** command sets the source IP address used by an SNMP server to send packets.

The **undo snmp-agent server-source** command restores the default source IP address used by an SNMP server to send packets.

By default, the SNMP server uses source IP address 0.0.0.0 to send packets.

Format

snmp-agent server-source { **-a** [**ipv6**] *source-ip-address* | **-i** [**ipv6**] *interface-type interface-number* }

undo snmp-agent [**ipv6**] **server-source**

Parameters

Parameter	Description	Value
ipv6	Specifies that the source IP address used by an SNMP server to send packets is an IPv6 address.	-
-a *source-ip-address*	Specifies the source IP address on the local device. A loopback interface address is recommended.	-
-i *interface-type interface-number*	Sets the loopback interface on the local device as the source interface. If no loopback interface exists on the device or the loopback interface does not have an IP address, the command fails.	-

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the default source IP address 0.0.0.0 is not changed, the device selects a source IP address according to routing entries to send packets. When an ACL is configured to filter incoming and outgoing packets on a device, the ACL rules are configured based on interface IP addresses, and packet filtering is affected by interface status. You can select a stable interface as the source interface, for example, the loopback interface. Setting the source or destination address in an ACL rule as a stable interface's address can simplify the configurations of ACL rules and security policies. In addition, packet filtering will not be affected by interface IP addresses and interface status, and device security is improved.

Precautions

- After the source IP address is specified for the SNMP server, the server address you entered when logging in to the server must be the same as that specified in this command; otherwise, you cannot log in to the server.
- If the SNMP service has been started, running this command will restart the SNMP service.

Example

Set LoopBack0 as the source interface of an SNMP server.

```
<Huawei> system-view
[Huawei] snmp-agent server-source -i loopback 0
Info: Succeeded in setting the source interface of the snmp-agent to LoopBack0
```

21.2 RMON and RMON2 Configuration Commands

21.2.1 display rmon alarm

Function

The **display rmon alarm** command displays information about RMON alarm function.

Format

display rmon alarm [*entry-number*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
entry-number	Displays information about the RMON alarm entry with the specified index. If no index is specified, information about all alarms is displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the RMON alarm thresholds using the **rmon alarm** command, you can run this command to view the configured alarm variables, sampling interval, thresholds, alarm triggering condition, and last sampled value.

Example

Display the RMON alarm configurations.

```
<Huawei> display rmon alarm
Alarm table 1 owned by creator is VALID.
  Samples delta value       : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval         : 5(sec)
  Rising threshold          : 1000 (linked with event 1)
  Falling threshold         : 100(linked with event 1)
  When startup enables      : risingOrFallingAlarm
  Latest value              : 0
```


Copyright © Huawei Technologies Co., Ltd.

Table 21-15 Description of the display rmon alarm command output

Item	Description
Alarm table *entry-number* owned by *owner* is *status*.	The current status of the alarm entry *entry-number* created by *owner* is *status*. • entry-number: alarm entry index, corresponding to the alarmIndex object in alarmTable. • owner: creator of the entry, corresponding to the alarmOwner object in alarmTable. • status: row status of the alarm entry with the specified index, corresponding to the alarmStatus in alarmTable. – UNDERCREATION: invalid – VALID: valid – INVALID: invalid due to hot swapping of the LPU
Samples delta value	Alarm variable, namely, monitored MIB object, corresponding to the alarmVariable object in alarmTable.
Sampling interval	Sampling interval, in seconds, corresponding to the alarmInterval object in alarmTable.
Rising threshold	Rising threshold of the alarm table, corresponding to the alarmRisingThreshold object in alarmTable. When the sampled value reaches or exceeds the rising threshold, an alarm is generated.
Falling threshold	Falling threshold of the alarm table, corresponding to the alarmFallingThreshold object in alarmTable. When the sampled value reaches or falls below the falling threshold, an alarm is generated.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
When startup enables	Condition that triggers alarms, corresponding to the alarmStartupAlarm object in alarmTable. When the sampled value exceeds the rising threshold or falls below the falling threshold, an alarm is generated. The values are: • risingOrFallingAlarm: generating an alarm when the sampled value exceeds the rising threshold or falls below the falling threshold • risingAlarm: generating an alarm when the sampled value exceeds the rising threshold • fallingAlarm: generating an alarm when the sampled value falls below the falling threshold
Latest value	Latest sampled value, corresponding to the alarmValue object in alarmTable.

Related Topics

21.2.11 rmon alarm

21.2.2 display rmon event

Function

The **display rmon event** command displays information about RMON events.

Format

display rmon event [*entry-number*]

Parameters

Parameter	Description	Value
entry-number	Displays the configuration of the RMON event with the specified index. If no index is specified, information about all events is displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

After configuring the trap or log function for RMON events, you can run this command to view the configured event description, whether events trigger traps and logs, and latest event.

Example

Display the RMON event configurations.

```
<Huawei> display rmon event
Event table 1 owned by Huawei is VALID.
  Description: null.
  Will cause log  when triggered, last triggered at 0days 00h:24m:10s.69th.
```

Table 21-16 Description of the display rmon event command output

Item	Description
Event table *entry-number* owned by *owner* is *status*.	The current status of the event entry *entry-number* created by *owner* is *status*. • entry-number: event entry index, corresponding to the eventIndex object in eventTable. • owner: creator of the entry, corresponding to the eventOwner object in eventTable. • status: row status of the event entry with the specified index, corresponding to the eventStatus in eventTable. – UNDERCREATION: invalid – VALID: valid – INVALID: invalid due to hot swapping of the LPU
Description	Event description, corresponding to the eventDescription object in eventTable.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Will cause log when triggered	Whether events trigger traps or logs, corresponding to the eventType object in eventTable. The actions associated with events are as follows: • none: no action is taken. • log: a log is recorded when an event is triggered. • trap: a trap is sent to the NMS when an event is triggered. • log-trap: a log is recorded and a trap is sent to the NMS when an event is triggered.
last triggered at	Latest event time, corresponding to the eventLastTimeSent object in eventTable.

Related Topics

21.2.12 rmon event

21.2.3 display rmon eventlog

Function

The **display rmon eventlog** command displays details about RMON event logs.

Format

display rmon eventlog [*entry-number*]

Parameters

Parameter	Description	Value
entry-number	Displays the log with the specified index. If no index is specified, information about all event logs is displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If you use the **rmon event** command to specify that a log is recorded for a certain event, the event record is stored in the LogTable. The command output includes event index, current event status, time the event triggers a log (calculated based on the number of seconds elapsed since system initialization or startup), and event description.

Example

Display the log of RMON event 1.

```
<Huawei> display rmon eventlog 1
Event table 1 owned by User is VALID.
  Generates eventLog 1.1 at 0days 00h:00m:07s.43th.
  Description: The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarm table 1, less than or equal to 100 with alarm value 0. Alarm sample type is delta.
  Generates eventLog 1.2 at 0days 00h:02m:26s.43th.
  Description: The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarm table 1, greater than or equal to 1000 with alarm value 10443. Alarm sample type is delta.
```

Table 21-17 Description of the display rmon eventlog command output

Item	Description
Event table *entry-number* owned by *owner* is *status*.	The current status of the event entry *entry-number* created by *owner* is *status*. • entry-number: event log entry index, corresponding to the logEventIndex object in LogTable. • owner: creator of the entry, corresponding to the eventOwner object in eventTable. • status: row status of the event entry with the specified index, corresponding to the eventStatus in eventTable. – UNDERCREATION: invalid – VALID: valid – INVALID: invalid due to hot swapping of the LPU
Generates eventLog at	Log creation time (time elapsed since system startup), corresponding to the logTime object in LogTable.
Description	Event description, corresponding to the logDescription object in LogTable.

Related Topics

21.2.2 display rmon event

21.2.12 rmon event

Copyright © Huawei Technologies Co., Ltd.

21.2.4 display rmon history

Function

The **display rmon history** command displays RMON history sampling information.

Format

display rmon history [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays RMON history sampling information on the specified Ethernet interface. If this parameter is not specified, RMON history sampling information on all interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring RMON history statistics on an interface using the **rmon history** command, the system samples packets on the interface periodically. The **display rmon history** command can display history sampling information, including the number of sampled packets, history sampling interval, latest sampling information, Ethernet interface usage, number of CRC error packets, and total number of packets.

Example

Display RMON history sampling information.

```
<Huawei> display rmon history
History control entry 1 owned by Creator is VALID
  Samples interface     : Ethernet2/0/0<ifEntry.402653698>
  Sampling interval     : 30(sec) with 10 buckets max
  Last Sampling time    : 0days 00h:09m:43s.00th
  Latest sampled values :
  octets              :645       , packets           :7
  broadcast packets   :7         , multicast packets :0
  undersize packets   :6         , oversize packets  :0
  fragments packets   :0         , jabbers packets   :0
  CRC alignment errors :0        , collisions        :0
  Dropped packet:     :0         , utilization       :0
```

Display RMON history sampling information on the specified interface.

```
<Huawei> display rmon history ethernet 2/0/0
History control entry 1 owned by Creator is VALID
```

 Copyright © Huawei Technologies Co., Ltd.

```
Samples interface     : Ethernet2/0/0<ifEntry.402653698>
Sampling interval     : 30(sec) with 10 buckets max
Last Sampling time    : 0days 00h:09m:43s.00th
Latest sampled values :
octets              :645       , packets           :7
broadcast packets   :7         , multicast packets :0
undersize packets   :6         , oversize packets  :0
fragments packets   :0         , jabbers packets   :0
CRC alignment errors :0        , collisions        :0
Dropped packet:     :0         , utilization       :0
History record:
Record No.1 (Sample time: 0days 00h:02m:30s.01th)
octets              :0         , packets           :0
broadcast packets   :0         , multicast packets :0
undersize packets   :0         , oversize packets  :0
fragments packets   :0         , jabbers packets   :0
CRC alignment errors :0        , collisions        :0
Dropped packet:     :0         , utilization       :0
```

Table 21-18 Description of the display rmon history command output

Item	Description
History control entry *entry-number* owned by *owner* is *status*.	The current status of the event entry *entry-number* created by *owner* is *status*. • entry-number: history control table entry index, corresponding to the historyControlIndex object in historyControlTable. • owner: creator of the entry, corresponding to the historyControlOwner object in historyControlTable. • status: row status of the history control table entry with the specified index, corresponding to the historyControlStatus in historyControlTable. – UNDERCREATION: invalid – VALID: valid – INVALID: invalid due to hot swapping of the LPU
Samples interface	Sampled interface.
Sampling interval	Sampling interval, in seconds, corresponding to the historyControlInterval object in historyControlTable. The system samples packets on the interface at this interval.
Last Sampling time	Latest sampling time, corresponding to the etherHistoryIntervalStart object in etherHistoryTable.
Latest sampled values	Latest sampling result.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
octets	Number of bytes received in a sampling interval, corresponding to the etherHistoryOctets object in etherHistoryTable.
packets	Number of packets received in a sampling interval, corresponding to the etherHistoryPkts object in etherHistoryTable.
broadcast packets	Number of broadcast packets received in a sampling interval, corresponding to the etherHistoryBroadcastPkts object in etherHistoryTable.
multicast packets	Number of multicast packets received in a sampling interval, corresponding to the etherHistoryMulticastPkts object in etherHistoryTable.
undersize packets	Number of undersize packets received in a sampling interval, corresponding to the etherHistoryUndersizePkts object in etherHistoryTable.
oversize packets	Number of large packets received in a sampling interval, corresponding to the etherHistoryOversizePkts object in etherHistoryTable.
fragments packets	Number of undersize and CRC error packets received in a sampling interval, corresponding to the etherHistoryFragments object in etherHistoryTable.
jabbers packets	Number of large and CRC error packets received in a sampling interval, corresponding to the etherHistoryJabbers object in etherHistoryTable.
CRC alignment errors	Number of CRC error packets received in a sampling interval, corresponding to the etherHistoryCRCAlignErrors object in etherHistoryTable.
collisions	Number of collision packets received in a sampling interval, corresponding to the etherHistoryCollisions object in etherHistoryTable.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dropped packet	Number of packets discarded in a sampling interval, corresponding to the etherHistoryDropEvents object in etherHistoryTable.
utilization	Bandwidth usage in a sampling interval, corresponding to the etherHistoryUtilization object in etherHistoryTable.
History record	History sampling result.

Related Topics

21.2.13 rmon history

21.2.5 display rmon prialarm

Function

The **display rmon prialarm** command displays information about RMON extended alarm function.

Format

display rmon prialarm [*entry-number*]

Parameters

Parameter	Description	Value
entry-number	Displays information about the RMON extended alarm entry with the specified index. If this parameter is not specified, all RMON extended alarm information is displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring RMON extended alarm function using the **rmon prialarm** command, you can run this command to view sampling interval, rising and falling thresholds, alarm triggering condition, and latest sampled value.

Copyright © Huawei Technologies Co., Ltd.

Example

Display the RMON extended alarm configurations.

```
<Huawei> display rmon prialarm
Prialarm table 1 owned by Huawei is VALID.
  Samples absolute value    : .1.3.6.1.2.1.16.1.1.1.6.1+.1.3.6.1.2.1.16.1.1.1.7.1
  Sampling interval         : 30(sec)
  Rising threshold          : 1000(linked with event 3)
  Falling threshold         : 100(linked with event 3)
  When startup enables      : risingOrFallingAlarm
  This entry will exist     : forever
  Latest value              : 557
```

Table 21-19 Description of the display rmon prialarm command output

Item	Description
Prialarm table *entry-number* owned by *owner* is *status*.	The current status of the extended alarm entry *entry-number* created by *owner* is *status*. ● entry-number: extended alarm entry. ● owner: creator of the entry. ● status: row status of the extended alarm entry with the specified index. – UNDERCREATION: invalid – VALID: valid – INVALID: invalid due to hot swapping of the LPU
Samples *type* value	The sampling type is *type*. The value of *type* can be: ● absolute: absolute value sampling ● delta: variable value sampling ● changeratio: change rate of sampled values (Change rate = Value change/Sampling interval) This field is followed by an alarm variable.
Sampling interval	Interval at which traffic is sampled.
Rising threshold	Alarm rising threshold.
Falling threshold	Alarm falling threshold.
linked with event *entry-number*	Associate with the row with index *entry-number*.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
When startup enables	Condition that triggers alarms (exceed the rising threshold or falls below the falling threshold). The values are: • risingOrFallingAlarm: generating an alarm when the sampled value exceeds the rising threshold or falls below the falling threshold • risingAlarm: generating an alarm when the sampled value exceeds the rising threshold • fallingAlarm: generating an alarm when the sampled value falls below the falling threshold
This entry will exist	Aging time of the extended alarm entry. An entry may be valid permanently or in a certain period.
Latest value	Latest sampling result.

Related Topics

21.2.14 rmon prialarm

21.2.6 display rmon statistics

Function

The **display rmon statistics** command displays RMON Ethernet statistics.

Format

display rmon statistics [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays RMON Ethernet statistics on the specified Ethernet interface. If this parameter is not specified, RMON Ethernet statistics on all interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After you configure Ethernet statistics using the **rmon statistics** command, the system collects packet statistics on Ethernet interfaces. The command output includes communication information generated since statistics function is enabled. The command output helps you locate faults.

When the device restarts, all statistics are cleared.

Example

Display RMON Ethernet statistics.

```
<Huawei> display rmon statistics
Statistics entry 1 owned by Creator is VALID.
  Interface : Ethernet2/0/0<ifEntry.402653698>
  Received  :
  octets              :142915224 , packets          :1749151
  broadcast packets   :11603     , multicast packets:756252
  undersize packets   :0         , oversize packets :0
  fragments packets   :0         , jabbers packets  :0
  CRC alignment errors:0         , collisions       :0
  Dropped packet (insufficient resources):1795
  Packets received according to length (octets):
  64     :150183    ,  65-127  :150183    ,  128-255  :1383
  256-511:3698      ,  512-1023:0         ,  1024-1518:0
```

Table 21-20 Description of the display rmon statistics command output

Item	Description
Statistics entry *entry-number* owned by *owner* is *status*.	The current status of the event entry *entry-number* created by *owner* is *status*. • entry-number: Ethernet statistics entry, corresponding to the etherStatsIndex object in etherStatsTable. • owner: creator of the entry, corresponding to the etherStatsOwner object in etherStatsTable. • status: row status of the Ethernet statistics entry with the specified index, corresponding to the etherStatsStatus in etherStatsTable. – UNDERCREATION: invalid – VALID: valid – INVALID: invalid due to hot swapping of the LPU
Interface	Interface where statistics are collected, corresponding to the etherStatsDataSource object in etherStatsTable, followed by the interface OID.
Received	Number of received packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
octets	Number of received octets.
packets	Number of received packets, corresponding to the etherStatsPkts object in etherStatsTable.
broadcast packets	Number of received broadcast packets, corresponding to the etherStatsBroadcastPkts object in etherStatsTable.
multicast packets	Number of received multicast packets, corresponding to the etherStatsMulticastPkts object in etherStatsTable.
undersize packets	Number of received undersize packets, corresponding to the etherStatsUndersizePkts object in etherStatsTable.
oversize packets	Number of received large packets, corresponding to the etherStatsOversizePkts object in etherStatsTable.
fragments packets	Number of received undersize and CRC error packets, corresponding to the etherStatsFragments object in etherStatsTable.
jabbers packets	Number of received large and CRC error packets, corresponding to the etherStatsJabbers object in etherStatsTable.
CRC alignment errors	Number of received CRC error packets, corresponding to the etherStatsCRCAlignErrors object in etherStatsTable.
collisions	Number of received collision packets, corresponding to the etherStatsCollisions object in etherStatsTable.
Dropped packet	Number of discarded packets, corresponding to the etherStatsDropEvents object in etherStatsTable.
Packets received according to length	Number of received packets with different lengths, corresponding to the etherStatsPkts64Octets, etherStatsPkts65to127Octets, etherStatsPkts128to255Octets, etherStatsPkts256to511Octets, etherStatsPkts512to1023Octets, and etherStatsPkts1024to1518Octets objects in etherStatsTable.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.2.15 rmon statistics

21.2.7 display rmon2 hlhostcontroltable

Function

The **display rmon2 hlhostcontroltable** command displays information about entries in hlHostControlTable.

Format

display rmon2 hlhostcontroltable [**index** *ctrl-index*] [**verbose**]

Parameters

Parameter	Description	Value
index *ctrl-index*	Indicates the entry index, which uniquely identifies an entry in the host control table.	The value is an integer that ranges from 1 to 65535.
verbose	Displays details about the host control table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you use the **rmon2 hlhostcontroltable** command to create a protocol directory table, you can run the **display rmon2 hlhostcontroltable** command to view the configurations.

If no entry index is specified, the configuration of the entire table is displayed.

Example

Display information about the entry with index 123 in the host control table.

```
<Huawei> display rmon2 hlhostcontroltable index 123
Abbreviation:
index - hlhostcontrolindex
datasource - hlhostcontroldatasource
droppedfrm - hlhostcontrolnldroppedframes
inserts - hlhostcontrolnlinserts
Deletes - hlHostControlNlDeletes
```


Copyright © Huawei Technologies Co., Ltd.

```
maxentries - hlhostcontrolnlmaxdesiredentries
status - hlhostcontrolstatus

index datasource              droppedfrm inserts    Deletes    maxentries      status
123   GE2/0/0                 0          0          0          50              active
```

Display detailed information about the entry with index 123 in the host control table.

```
<Huawei> display rmon2 hlhostcontroltable index 123 verbose
Abbreviation:
index - hlhostcontrolindex
datasource - hlhostcontroldatasource
droppedfrm - hlhostcontrolnldroppedframes
inserts - hlhostcontrolnlinserts
Deletes - hlHostControlNlDeletes
maxentries - hlhostcontrolnlmaxdesiredentries
owner - hlhostcontrolowner
status - hlhostcontrolstatus

index      :   123
datasource :   GigabitEthernet2/0/0
droppedfrm :   0
inserts    :   7
Deletes    :   0
maxentries :   100
owner      :   china
status     :   active
```

Table 21-21 Description of the **display rmon2 hlhostcontroltable** command output

Item	Description
index	Index of hlHostControlTable.
datasource	Source interface of data.
droppedfrm	Number of the frames that are received on the statistics interface but not added into nlHost entries.
inserts	Times add nlHost entries are added to nlHostTable.
Deletes	Times nlHost entries are deleted from nlHostTable.
maxentries	Maximum number of entries that nlHostTable contains.
owner	Owner of entries.
status	Status of entries in the hlHostControlTable. • active: running normally • notinservice: invalid

Related Topics

21.2.16 rmon2 hlhostcontroltable

Copyright © Huawei Technologies Co., Ltd.

21.2.8 display rmon2 nlhosttable

Function

The **display rmon2 nlhosttable** command displays information about entries in the nlHostTable.

Format

display rmon2 nlhosttable [**hostcontrolindex** *ctrl-index*] [**hostaddress** *ip-address*]

Parameters

Parameter	Description	Value
hostcontrolindex *ctrl-index*	Specifies the index number. A *ctrl-index* uniquely identifies an entry in the hlHostControlTable.	It is an integer ranging from 1 to 65535.
hostaddress *ip-address*	Checks the traffic on a specified host.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After statistics function is configured on an interface, you can view traffic statistics using this command. A maximum of 5000 rows can be displayed for each protocol on an interface.

Example

Display information about the entry with index 1 in the host table.

```
<Huawei> display rmon2 nlhosttable hostcontrolindex 1 hostaddress 10.110.94.177
Abbreviation:
HIdx - hlHostControlIndex
Addr - nlHostAddress
InPkts - nlHostInPkts
OutPkts - nlHostOutPkts
InOctes - nlHostInOctets
OutOctes - nlHostOutOctets
OutMac - nlHostOutMacNonUnicastPkts
HIdx   Addr            InPkts     OutPkts    InOctes    OutOctes   OutMac
1      10.110.94.177    4          5          216        483
```

 Copyright © Huawei Technologies Co., Ltd.

Table 21-22 Description of the display rmon2 nlhosttable command output

Item	Description
HIdx	Index of the host control table.
Addr	Host address. It is the source address of the incoming IP packets on the monitored interface and destination address of the outgoing IP packets on the interface.
InPkts	Number of incoming packets on the monitored interface.
OutPkts	Number of outgoing packets on the monitored interface.
InOctes	Number of incoming bytes on the monitored interface.
OutOctes	Number of outgoing bytes on the monitored interface.
OutMac	Number of outgoing non-unicast packets on the monitored interface.

21.2.9 display rmon2 protocoldirtable

Function

The **display rmon2 protocoldirtable** command displays all entries in the protocolDirTable.

Format

display rmon2 protocoldirtable

Parameters

None

Views

All views

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After you use the **rmon2 protocoldirtable** command to configure statistics on IP packets, you can run the **display rmon2 protocoldirtable** command to view the configurations.

Example

Display entries in the protocolDirTable.

```
<Huawei> display rmon2 protocoldirtable
protocolDirId              :  8.0.0.0.1.0.0.8.0
protocolDirParameters      :  2.0.0
protocolDirLocalIndex      :  2
protocolDirDescr           :  IP
protocolDirAddressMapConfig:  notsupported
protocolDirHostConfig      :  supportedon
protocolDirMatrixConfig    :  notsupported
protocolDirOwner           :  china
protocolDirStatus          :  active
```

Table 21-23 Description of the display rmon2 protocoldirtable command output

Item	Description
protocolDirId	Protocol directory ID. Currently, RMON2 only supports IP protocol, so the protocol directory ID is fixed at 8.0.0.0.1.0.0.8.0.
protocolDirParameters	Protocol directory parameter. The value is fixed at 2.0.0.
protocolDirLocalIndex	Local protocol directory index.
protocolDirDescr	Protocol directory description.
protocolDirAddressMapConfig	Whether protocol directory address mapping is supported. This function is not supported currently.
protocolDirHostConfig	• notsupported: The device does not monitor the network-layer host table of the protocol, and this value cannot be changed. • supportedon: The device can monitor the network-layer host table of the protocol, and the monitoring function is enabled. • supportedoff: The device can monitor the network-layer host table of the protocol, but the monitoring function is disabled.
protocolDirMatrixConfig	Whether protocol directory matrix is supported. This function is not supported currently.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
protocolDirOwner	Protocol directory owner.
protocolDirStatus	Protocol directory status. • active: running normally • not in service: invalid

Related Topics

21.2.17 rmon2 protocoldirtable

21.2.10 display snmp-agent trap feature-name rmon all

Function

The **display snmp-agent trap feature-name rmon all** command displays the status of all traps about the RMON module.

Format

display snmp-agent trap feature-name rmon all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the status of all traps about the RMON module.

```
<Huawei> display snmp-agent trap feature-name rmon all
-------------------------------------------------------------------------------
Feature name: RMON
Trap number : 4
-------------------------------------------------------------------------------
Trap name                 Default switch status   Current switch status
risingalarm               on                      on
fallingalarm              on                      on
rmon_pri_risingalarm          on                      on
rmon_pri_fallingalarm         on                      on
```

 Copyright © Huawei Technologies Co., Ltd.

Table 21-24 Description of the display snmp-agent trap feature-name rmon all command output

Item	Description
Feature name	Name of the module to which a trap message belongs.
Trap number	Number of trap messages.
Trap name	Name of a trap message of the RMON module.
Default switch status	Default status of the trap function: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.
Current switch status	Current status of the trap function: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.
risingalarm	Indicates that the current sampled value is greater than or equal to the set threshold specified by the alarm table.
fallingalarm	Indicates that the current sampled value is less than or equal to the set threshold specified by the alarm table.
rmon_pri_risingalarm	Indicates that the current sampled value is greater than or equal to the set threshold specified by the pri_alarm table.
rmon_pri_fallingalarm	Indicates that the current sampled value is less than or equal to the set threshold specified by the pri_alarm table.

Related Topics

21.2.19 snmp-agent trap enable feature-name rmon

21.2.11 rmon alarm

Function

The **rmon alarm** command adds an entry to the alarm table.

The **undo rmon alarm** command deletes an entry from the alarm table.

Format

rmon alarm *entry-number alarm-OID sampling-time* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *owner-name*]

Copyright © Huawei Technologies Co., Ltd.

undo rmon alarm *entry-number*

Parameters

Parameter	Description	Value
entry-number	Specifies the index of the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.
alarm-OID	Specifies the alarm OID.	The name is a string of 1 to 256 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
sampling-time	Specifies the sampling interval.	The value is an integer that ranges from 5 to 65535, in seconds.
absolute	Indicates that the sample type is absolute. The value is the sampled value at the end of the period.	-
changeratio	Indicates that the sample type is changeratio. The value is Changing value/Sampling interval.	-
delta	Indicates that the sample type is delta. The value is the difference between the samples at the beginning and end of the period.	-
rising-threshold *threshold-value1*	Specifies the rising threshold of sampled value.	The value is an integer that ranges from 1 to 2147483647.
event-entry1	Indicates the event index corresponding to the rising threshold.	The value is an integer that ranges from 1 to 65535.
falling-threshold *threshold-value2*	Specifies the falling threshold of sampled value.	The value is an integer that ranges from 0 to 2147483646.
event-entry2	Indicates the event index corresponding to the falling threshold.	The value is an integer that ranges from 1 to 65535.
owner *owner-name*	Indicates the owner of the alarm.	The name is a string of 1 to 127 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor system running status, run the **rmon alarm** command to configure an alarm table and add an entry to the alarm table. After the command is executed, the RMON alarm function is enabled. The system obtains information about the monitored object at the specified interval, and compares the obtained value with the configured threshold. Then the system triggers the event according to the following table, and records log or sends a trap to the NMS.

Situation	Action
The sampled value is larger than or equal to the configured rising threshold *threshold-value1*.	Trigger *event-entry1*.
The sampled value is smaller than or equal to the configured falling threshold *threshold-value2*.	Trigger *event-entry2*.

Prerequisites

Before configuring alarm function for the specified object, run the **rmon event** command to define the associated events.

If the alarm variables configured in RMON alarm function are MIB variables defined in the statistics group or history group, the Ethernet statistics function or history statistics function must be configured on the monitored Ethernet interface first. Otherwise, alarm entries cannot be created.

Example

Monitor alarm thresholds for etherStatsBroadcastPkts (alarm OID is 1.3.6.1.2.1.16.1.1.1.6.1): Set the sampling interval to 30 seconds and sample type to absolute. When the sampled value reaches or exceeds 500, event 1 is triggered. When the sampled value reaches or falls below 100, event 2 is triggered. The owner is **creator**.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] rmon statistics 1 owner creator
[Huawei-Ethernet2/0/0] quit
[Huawei] rmon event 1 log
[Huawei] rmon event 2 trap public
[Huawei] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 30 absolute rising-threshold 500 1 falling-threshold 100
2 owner creator
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.2.1 display rmon alarm

21.2.12 rmon event

Function

The **rmon event** command adds an entry to the event table.

The **undo rmon event** command deletes an entry from the event table.

Format

rmon event *entry-number* [**description** *string*] { **log** | **trap** *object* | **log-trap** *object* | **none** } [**owner** *owner-name*]

undo rmon event *entry-number*

Parameters

Parameter	Description	Value
entry-number	Specifies the index of the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.
description *string*	Specifies the event description.	The value is a string of 1 to 127 characters.
log	Records a log for the event.	-
trap	Sends a trap to the NMS.	-
object	Specifies the community name of the NMS receiving the trap.	The value is a string of 1 to 127 characters.
log-trap	Records a log and sends a trap to the NMS for the event.	-
none	Indicates that no action is taken for the event.	-
owner *owner-name*	Indicates the creator of the event entry.	The name is a string of 1 to 127 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

This command specifies whether to record a log or send a trap for events. When an error occurs in the system, the RMON alarm function triggers the corresponding event. You can run the **rmon event** command to configure an event table and add an entry to the table. The entry specifies whether to record a log or send a trap to the NMS for the event.

Prerequisites

The **rmon alarm** command is executed to configure the alarm objects. Otherwise, no alarm will trigger the event.

Example

Send a trap to the NMS for event 10.

```
<Huawei> system-view
[Huawei] rmon event 10 trap public
```

Related Topics

21.2.2 display rmon event

21.2.13 rmon history

Function

The **rmon history** command adds an entry to the history control table.

The **undo rmon history** command deletes an entry from the history control table.

Format

rmon history *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *owner-name*]

undo rmon history *entry-number*

Parameters

Parameter	Description	Value
entry-number	Specifies the index of the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.
buckets *number*	Indicates the maximum number of records in the history control table.	The value is an integer that ranges from 1 to 10.
interval *sampling-interval*	Specifies the sampling interval.	The value is an integer that ranges from 5 to 3600, in seconds.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
owner *owner-name*	Indicates the owner of the entry in the history control table.	The name is a string of 1 to 127 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

Ethernet interface view, GE interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect statistics on the specified interface at an interval and save the statistics for future retrieval, run the **rmon history** command to configure a history control table and add an entry to the table. The system can periodically collect statistics on each type of traffic, including bandwidth usage, number of error packets, and total number of packets.

Precautions

The number of stored records is determined by the **buckets** *number* parameter. When the number of records in the table reaches the maximum, the system overwrites the old records with new ones. Statistics include the number of packets, broadcast packets, and multicast packets received by the interface within a sampling interval. You can run the **display rmon history** command to view history sampling results.

Example

Configure a history control table and add an entry with index 1 to the table. Set the maximum number of entries in the table to 10, sampling interval to 5 seconds, and creator to **user1**.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] rmon history 1 buckets 10 interval 5 owner user1
```

Related Topics

21.2.4 display rmon history

21.2.14 rmon prialarm

Function

The **rmon prialarm** command adds an entry to the extended alarm table.

Copyright © Huawei Technologies Co., Ltd.

The **undo rmon prialarm** command deletes an entry from the extended alarm table.

Format

rmon prialarm *entry-number prialarm-formula description-string sampling-interval* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **cycle** *entry-period* | **forever** } [**owner** *owner-name*]

undo rmon prialarm *entry-number*

Parameters

Parameter	Description	Value
entry-number	Specifies the index of the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.
prialarm-formula	Specifies the formula for calculating an alarm variable. The alarm variable in the formula is identified by an OID. The OID value starts with a dot, for example, (.1.3.6.1.2.1.2.1.10.1)*8. The calculation formula is defined by user. The calculation result is a long integer. Ensure that the length of calculation result in each step cannot exceed the limit; otherwise, the calculation result is incorrect.	The value is a string of 1 to 256 characters.
description-string	Specifies the alarm description.	The value is a string of 1 to 256 characters.
sampling-interval	Specifies the sampling interval.	The value is an integer that ranges from 10 to 65535, in seconds.
absolute	Indicates that the sample type is absolute. The value is the sampled value at the end of the period.	-
changeratio	Indicates that the sample type is changeratio. The value is Changing value/Sampling interval.	-
delta	Indicates that the sample type is delta. The value is the difference between the samples at the beginning and end of the period.	-
rising-threshold *threshold-value1*	Specifies the alarm rising threshold.	The value is an integer that ranges from 1 to 2147483647.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
event-entry1	Indicates the entry number of the event corresponding to the rising threshold in the event table.	The value is an integer that ranges from 1 to 65535.
falling-threshold *threshold-value2*	Specifies the alarm falling threshold.	The value is an integer that ranges from 0 to 2147483646.
event-entry2	Indicates the entry number of the event corresponding to the falling threshold in the event table.	The value is an integer that ranges from 1 to 65535.
entrytype	Indicates the lifetime type of an alarm entry.	-
cycle *entry-period*	Indicates the lifetime of an alarm entry.	The value is an integer that ranges from 11 to 2147483646.
forever	Indicates that the alarm entry is valid permanently.	-
owner *owner-name*	Indicates the owner of the extended alarm variable.	The value is a string of 1 to 127 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The extended alarm function can compute the alarm variables and compare the result with the specified threshold.

After the extended alarm function is enabled, the system performs the following operations:

1. Samples the alarm variables in the extended alarm formula at the specified sampling interval.
2. Calculates the sampled value using the defined formula.
3. Compares the calculation result with the thresholds and takes actions according to the following table.

 Copyright © Huawei Technologies Co., Ltd.

Situation	Action
The sampled value is larger than or equal to the configured rising threshold *threshold-value1*.	Trigger *event-entry1*.
The sampled value is smaller than or equal to the configured falling threshold *threshold-value2*.	Trigger *event-entry2*.

To use more alarm functions, run the **rmon prialarm** command to configure the extended alarm table and add an entry to the table.

Prerequisites

Before configuring extended alarm function for the specified object, run the **rmon event** command to define the associated events. Otherwise, events cannot be triggered even if alarms are generated. When the sampled value exceeds the rising threshold or falls below the falling threshold, whether to record a log or send a trap to the NMS is determined by the **rmon event** command.

Example

Monitor broadcast and multicast packets: Set the sampling interval to 10 seconds and sample type to absolute. Trigger event 3 when the sample value reaches or exceeds 100000 and when the sample value reaches or falls below 100. Set the lifetime of the entry to forever and the owner to **Huawei**.

```
<Huawei> system-view
[Huawei] rmon prialarm 1 .1.1.3.6.1.2.1.16.1.1.1.6.1+.1.3.6.1.2.1.16.1.1.1.7.1 sumofbroadandmulti 10 absolute rising-threshold 100000 3 falling-threshold 100 3 entrytype forever owner Huawei
```

Related Topics

21.2.5 display rmon prialarm

21.2.15 rmon statistics

Function

The **rmon statistics** command adds an entry to the statistics table.

The **undo rmon statistics** command deletes an entry from the statistics table.

Format

rmon statistics *entry-number* [**owner** *owner-name*]

undo rmon statistics *entry-number*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
entry-number	Indicates the row index corresponding to the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.
owner *owner-name*	Indicates the owner name.	The name is a string of 1 to 127 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

Ethernet interface view, GE interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To keep collecting statistics on the current interface, run the **rmon statistics** command to configure a statistics table and add an entry to the table. This command monitors usage of Ethernet interfaces and collects statistics on errors, including the number of collision packets, CRC error packets, undersize and large packets, timeout packets, fragments, broadcast packets, multicast packets, and unicast packets.

Prerequisites

The **rmon-statistics enable** command is executed to enable RMON statistics function on the interface. If the command is not executed, the statistics result is 0.

Example

Configure a statistics table on Ethernet2/0/0 and add an entry with index 20 to the table.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] rmon statistics 20 owner creater
```

Related Topics

21.2.6 display rmon statistics

21.2.18 rmon-statistics enable

Copyright © Huawei Technologies Co., Ltd.

21.2.16 rmon2 hlhostcontroltable

Function

The **rmon2 hlhostcontroltable** command creates or changes an entry in the hlHostControlTable.

The **undo rmon2 hlhostcontroltable** command deletes an entry from the hlHostControlTable or from the whole table.

Format

rmon2 hlhostcontroltable index *ctrl-index* [**datasource interface** *interface-type interface-number*] [**maxentry** *maxentry-value*] [**owner** *owner-name*] [**status** { **active** | **inactive** }]

undo rmon2 hlhostcontroltable [**index** *ctrl-index*]

Parameters

Parameter	Description	Value
ctrl-index	Indicates the entry index, which uniquely identifies an entry in the host control table.	The value is an integer that ranges from 1 to 65535.
datasource interface *interface-type interface-number*	Identifies an interface and a subnet, corresponding to hlHostControlDataSource. The parameter value, namely, the interface index, is the data source defining the entry. In this command, the data source is represented by interface type and number.	-
maxentry *maxentry-value*	Indicates the maximum number of entries in the host table.	The value is an integer that ranges from 1 to 100000. The default value is 50. If the host table contains too many entries, system performance is degraded. The default settings of host table are recommended.
owner *owner-name*	Indicates the owner.	The value is a string of 1 to 127 characters and cannot be empty.
status	Indicates the status of an entry in the host control table, corresponding to hlHostControlStatus.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
active	Indicates that the hlHostControlStatus value in the host control table is active and this entry is available.	-
inactive	Indicates that the hlHostControlStatus value in the host control table is not in service and this entry is inactive and unavailable.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor traffic on the subnet connected to an interface of the managed device, run the **rmon2 hlhostcontroltable** command and specify the interface.

Precautions

When creating an entry, specify the **datasource interface** parameter to identify the interface, which specifies the subnet. The parameter value, namely, the interface index, is the data source defining the entry. Enter the interface type and number in the command. Only one entry can be created for each interface in the host control table.

The parameter **status** in the **display rmon2 hlhostcontroltable** command output matches the hlhostcontrolstatus value, which indicates the entry status.

- When the hlhostcontrolstatus value is set to **inactive**, all related entries in the host table are deleted automatically.
- When the hlhostcontrolstatus value is set to **active**, you cannot change the hlhostcontroldatasource and hlhostcontrolnlmaxdesiredentries values.
- If an interface that corresponds to the hlhostcontroldatasource in an entry is deleted, the entry is deleted at the same time.

Example

Create an entry in the host control table.

```
<Huawei> system-view
[Huawei] rmon2 hlhostcontroltable index 1 datasource interface ethernet 2/0/0 maxentry 100 owner huawei status active
```

Set the hlHostControlStatus value in the host control table to **not in service**.

```
<Huawei> system-view
[Huawei] rmon2 hlhostcontroltable index 1 status inactive
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.2.7 display rmon2 hlhostcontroltable

21.2.17 rmon2 protocoldirtable

Function

The **rmon2 protocoldirtable** command creates or modifies an entry in the protocolDirTable.

The **undo rmon2 protocoldirtable** command deletes an entry from the protocolDirTable. If optional parameters are not specified, the entire table is deleted.

Format

rmon2 protocoldirtable protocoldirid *protocol-id* **parameter** *parameter-value* [**descr** *description-string*] [**host** { **notsupported** | **supportedon** | **supportedoff** }] [**owner** *owner-name*] [**status** { **active** | **inactive** }]

undo rmon2 protocoldirtable [**protocoldirid** *protocol-id* **parameter** *parameter-value*]

Parameters

Parameter	Description	Value
protocol-id	Indicates the protocol ID. Only IP protocol is supported currently.	The value is fixed at 8.0.0.0.1.0.0.8.0.
parameter *parameter-value*	Indicates the protocol parameter.	The value is fixed at 2.0.0.
descr *description-string*	Indicates the description of the protocol directory table.	The value is a string of 1 to 64 characters.
host	Indicates the configuration of protocol directory host, corresponding to protocolDirHostConfig in the **display rmon2 protocoldirtable** command output.	-
notsupported	Indicates that the device does not monitor the network-layer host table of the protocol, and this value cannot be changed.	-
supportedon	Indicates that the device can monitor the network-layer host table of the protocol, and the monitoring function is enabled.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
supportedoff	Indicates that the device can monitor the network-layer host table of the protocol, but the monitoring function is disabled.	-
owner *owner-name*	Indicates the owner.	The value is a string of 1 to 127 characters.
status	Indicates the entry status, corresponding to the protocolDirStatus value in the **display rmon2 protocoldirtable** command output.	-
active	Indicates that the protocolDirStatus value in the host control table is active and this entry is available.	-
inactive	Indicates that the protocolDirStatus value in the host control table is not in service and this entry is inactive and unavailable.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor statistics on IP packets, run this command.

RMON2 supports only statistics on IP packets on an Ethernet interface. A protocol occupies an entry, so there is only one entry in the table.

Precautions

When running the **rmon2 protocoldirtable** command, you must set the description and protocols supported by the host. That is, the **descr** and **host** parameters are mandatory.

The parameter **status** in the **display rmon2 protocoldirtable** command output matches the protocoldirStatus value, which indicates the entry status.

- When the **status** parameter is set to **active**, the **descr** value cannot be modified. The value of **host** (corresponding to the protocolDirHostConfig value, indicating the protocol directory host configuration) can be modified. This parameter indicates whether to monitor the network-layer host table of the protocol.

 Copyright © Huawei Technologies Co., Ltd.

  - If the **host** value is set to **notsupported**, the **host** value cannot be modified.
  - If the **host** value is not **notsupported**, the value can be switched between **supportedon** and **supportedoff**.
  - When the **host** value is changed from **supportedon** to **supportedoff**, the corresponding entry in the host control table is deleted.
- When the status is **inactive**, all related entries in the host table are deleted.

Example

Create an entry in the protocol directory table.

```
<Huawei> system-view
[Huawei] rmon2 protocoldirtable protocoldirid 8.0.0.0.1.0.0.8.0 parameter 2.0.0 descr huawei host supportedon owner huawei status active
```

Set the protocolDirStatus value in the protocol directory table to not in service.

```
<Huawei> system-view
[Huawei] rmon2 protocoldirtable protocoldirid 8.0.0.0.1.0.0.8.0 parameter 2.0.0 status inactive
```

Set the protocolDirHostConfig value in the protocol directory table to supportedon.

```
<Huawei> system-view
[Huawei] rmon2 protocoldirtable protocoldirid 8.0.0.0.1.0.0.8.0 parameter 2.0.0 host supportedon
```

Related Topics

21.2.9 display rmon2 protocoldirtable

21.2.18 rmon-statistics enable

Function

The **rmon-statistics enable** command enables RMON statistics function on an interface.

The **undo rmon-statistics** command disables RMON statistics function on an interface.

By default, RMON statistics function is disabled on interfaces.

Format

rmon-statistics enable

undo rmon-statistics

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

If the statistics function is not enabled on an interface, statistics in the statistics table and history table are 0.

Example

Enable RMON statistics function on Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] rmon-statistics enable
```

Related Topics

21.2.15 rmon statistics

21.2.19 snmp-agent trap enable feature-name rmon

Function

The **snmp-agent trap enable feature-name rmon** command enables the alarm function for the RMON module.

The **undo snmp-agent trap enable feature-name rmon** command disables the alarm function for the RMON module.

By default, the alarm function is enabled for the RMON module.

Format

snmp-agent trap enable feature-name rmon [**trap-name** { **fallingalarm** | **risingalarm** | **rmon_pri_fallingalarm** | **rmon_pri_risingalarm** }]

undo snmp-agent trap enable feature-name rmon [**trap-name** { **fallingalarm** | **risingalarm** | **rmon_pri_fallingalarm** | **rmon_pri_risingalarm** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the alarm function for the specified event. If no event type is specified using the **trap-name** parameter, all types of alarms are enabled or disabled for the RMON module.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
fallingalarm	Indicates that the current sampled value is smaller than or equal to the threshold configured in the alarmTable.	-
risingalarm	Indicates that the current sampled value is larger than or equal to the threshold configured in the alarmTable.	-
rmon_pri_fallingalarm	Indicates that the current sampled value is smaller than or equal to the threshold configured in the prialarmTable.	-
rmon_pri_risingalarm	Indicates that the current sampled value is larger than or equal to the threshold configured in the prialarmTable.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

A device managed by the NMS can send traps to the NMS if the alarm function is enabled for the RMON module on the device. By default, all alarms for the RMON module are enabled. If only one or some event alarms need to be enabled, run the **snmp-agent trap enable feature-name rmon trap-name** command.

Example

Enable the fallingalarm for the RMON module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name rmon trap-name fallingalarm
```

21.3 TCP FPM Configuration Commands

21.3.1 display tcp fpm session

Function

The **display tcp fpm session** command displays TCP FPM statistics.

Copyright © Huawei Technologies Co., Ltd.

Format

display tcp fpm session { **all** | **number** }

Parameters

Parameter	Description	Value
all	Displays all TCP FPM statistics.	-
number	Indicates the number of sessions involved in TCP FPM statistics collection.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can display TCP FPM statistics, including network delay and packet loss rate, which are the reference for network optimization.

Example

Display all TCP FPM statistics.

```
<Huawei> display tcp fpm session all
Index DstIP(Port)          SrcIP(Port)          Loss(%)  SND  CND  RT   Application
1 10.1.1.3(2053)           10.1.3.2(3351)         0       12   4    0     FTP
```

Display the number of entries of which the TCP FPM statistics are displayed.

```
<Huawei> display tcp fpm session number
 TCP fpm session number : 2
```

Table 21-25 Description of the **display tcp fpm session** command output

Item	Description
Index	Index of a session involved in TCP FPM statistics collection.
DstIP(Port)	IP address and port number of the application server.
SrcIP(Port)	IP address and port number of the application client.
Loss(%)	Packet loss rate.
CND	Network time on the client.
SND	Network time on the server.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
RT	Response time of the router.
Application	Application type.
TCP fpm session number	Number of sessions involved in TCP FPM statistics collection.

21.3.2 reset tcp fpm session all

Function

The **reset tcp fpm session all** command clears TCP FPM statistics.

Format

reset tcp fpm session all

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To understand the quality of the network running TCP applications, clear existing TCP FPM statistics first, and then collect new statistics. From the latest statistics, you can know the network status in real time.

Precautions

Statistics cannot be restored after being cleared. Exercise caution when you run the following commands.

Example

Clear TCP FPM statistics.

```
<Huawei> system-view
[Huawei] reset tcp fpm session all
 Reset tcp fpm session success .
```

 Copyright © Huawei Technologies Co., Ltd.

21.3.3 pm report tcp fpm enable

Function

The **pm report tcp fpm enable** command enables the function of reporting TCP FPM statistics to the controller.

The **undo pm report tcp fpm enable** command disables the function of reporting TCP FPM statistics to the controller.

By default, TCP FPM statistics are not reported to the controller.

Format

pm report tcp fpm enable

undo pm report tcp fpm enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

TCP FPM statistics can be displayed in two methods:

- CLI: Run the
  display tcp fpm session
  command to view TCP FPM statistics.
- Controller: Display TCP FPM statistics on the GUI.

If you want to view statistics on the controller, enable the function of reporting TCP FPM statistics to the controller.

Precautions

This method can be used only in the SD-WAN solution, in which a controller is deployed.

Example

Enable the function of reporting TCP FPM statistics to the controller.

```
<Huawei> system-view
[Huawei] pm report tcp fpm enable
```

 Copyright © Huawei Technologies Co., Ltd.

21.3.4 tcp fpm enable

Function

The **tcp fpm enable** command enables the TCP FPM function.

The **undo tcp fpm enable** command disables the TCP FPM function.

By default, the TCP FPM function is disabled.

Format

tcp fpm enable

undo tcp fpm enable

Parameters

None

Views

Interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the TCP FPM function is enabled, the router can collect network performance statistics of TCP applications, such as delay and packet loss rate. You can optimize the network based on the network performance.

Precautions

Ethernet interfaces do not support this command when working as Layer 2 interfaces. Therefore, the interfaces must be added to VLANIF interfaces or the interface mode must be switched to Layer 3.

Example

Enable the TCP FPM function.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] tcp fpm enable
```

21.3.5 tcp fpm report time

 Copyright © Huawei Technologies Co., Ltd.

Function

The **tcp fpm report time** command sets the interval for reporting TCP FPM statistics to the controller.

The **undo tcp fpm report time** command sets the interval for reporting TCP FPM statistics to the controller to the default value.

By default, the interval for reporting TCP FPM statistics to the controller is 60s.

Format

tcp fpm report time *time*

undo tcp fpm report time

Parameters

Parameter	Description	Value
time	Specifies the interval for reporting TCP FPM statistics to the controller.	The value is an integer that ranges from 5 to 86400, in seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the router sends statistics on TCP applications, such as delay and packet loss rate, to the controller at an interval of 60s. You can change the interval if needed.

Example

Set the interval for reporting TCP FPM statistics to the controller to 100s.

```
<Huawei> system-view
[Huawei] tcp fpm report time 100
```

21.4 IP FPM Configuration Commands

21.4.1 authentication-mode (IPFPM-DCP view)

Function

The **authentication-mode** command configures the authentication mode and password for a Data Collecting Point (DCP).

Copyright © Huawei Technologies Co., Ltd.

The **undo authentication-mode** command deletes the authentication mode and password of a DCP.

By default, no authentication mode or password is configured for a DCP.

Format

authentication-mode hmac-sha256 key-id *key-id* [**cipher**] *password*

undo authentication-mode hmac-sha256

Parameters

Parameter	Description	Value
hmac-sha256	Indicates the HMAC-SHA256 authentication algorithm to be used for packets sent from a DCP to an MCP.	-
key-id *key-id*	Specifies the key ID for the authentication password of a DCP.	The value is an integer ranging from 1 to 64.
cipher	Indicates that the authentication password is displayed in ciphertext.	-
password	Specifies the authentication password of a DCP.	The value is a string of characters. • The value ranges from 1 to 255 for simple passwords. • The value ranges from 32 to 392 for ciphertext passwords.

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enhance network security and performance statistics reliability, run the **authentication-mode** command so that authentication is performed during IP FPM performance statistics. An MCP and its associated DCPs must have the same

Copyright © Huawei Technologies Co., Ltd.

authentication mode and password configured. The MCP processes packets only from the authenticated DCPs.

Prerequisites

The **nqa ipfpm dcp** command has been run to enable DCP globally.

Precautions

IP FPM supports only the HMAC-SHA256 authentication algorithm.

Example

Configure the authentication mode and password for a DCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-ipfpm-dcp] authentication-mode hmac-sha256 key-id 1 cipher Huawei-123
```

21.4.2 authentication-mode (IPFPM-MCP view)

Function

The **authentication-mode** command configures the authentication mode and password for a Measurement Control Point (MCP) in the IP Flow Performance Measurement (IP FPM) model.

The **undo authentication-mode** command deletes the authentication mode and password of an MCP in the IP FPM model.

By default, no authentication mode or password is configured for an MCP in the IP FPM model.

Format

authentication-mode hmac-sha256 key-id *key-id* [**cipher**] *password*

undo authentication-mode hmac-sha256 key-id *key-id*

Parameters

Parameter	Description	Value
hmac-sha256	Indicates the HMAC-SHA256 authentication algorithm to be used for packets sent from a DCP to an MCP.	-
key-id *key-id*	Specifies the key ID for the authentication password of an MCP.	The value is an integer ranging from 1 to 64.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher	Indicates that the authentication password is displayed in ciphertext.	-
password	Specifies the authentication password of an MCP.	The value is a string of case-sensitive characters without spaces. • The value ranges from 1 to 255 for simple passwords. • The value ranges from 32 to 392 for ciphertext passwords.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enhance network security and performance statistics reliability, run the **authentication-mode** command so that authentication is performed during IP FPM performance statistics. An MCP and its associated DCPs must have the same authentication mode and password configured. The MCP processes packets only from the authenticated DCPs.

Precautions

IP FPM supports only the HMAC-SHA256 authentication algorithm.

The authentication mode and password configured on an MCP must be the same as those configured on the DCPs associated with this MCP. Otherwise, the MCP cannot process the statistics reported by the DCPs.

Example

Configure the authentication mode and password for an MCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
[Huawei-nqa-ipfpm-mcp] authentication-mode hmac-sha256 key-id 1 Huawei-123
```

 Copyright © Huawei Technologies Co., Ltd.

21.4.3 authentication-mode (IPFPM-DCP instance view)

Function

The **authentication-mode** command configures the authentication mode and password for an IP FPM instance.

The **undo authentication-mode** command deletes the authentication mode and password of an IP FPM instance.

By default, no authentication mode or password is configured for an IP FPM instance.

Format

authentication-mode hmac-sha256 key-id *key-id* [**cipher**] *password*

undo authentication-mode hmac-sha256

Parameters

Parameter	Description	Value
hmac-sha256	Indicates the HMAC-SHA256 authentication algorithm to be used for packets sent from a DCP to an MCP.	-
key-id *key-id*	Specifies the key ID for the authentication password of an IP FPM instance.	The value is an integer ranging from 1 to 64.
cipher	Indicates that the authentication password is displayed in ciphertext.	-
password	Specifies the authentication password of an IP FPM instance.	The value is a string of case-sensitive characters without spaces. • The value ranges from 1 to 255 for simple passwords. • The value ranges from 32 to 392 for ciphertext passwords.

Views

IPFPM-DCP instance view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enhance network security and performance statistics reliability, run the **authentication-mode** command so that authentication is performed during IP FPM performance statistics. An MCP and its associated DCPs must have the same authentication mode and password configured. The MCP processes packets only from the authenticated DCPs.

Precautions

IP FPM supports only the HMAC-SHA256 authentication algorithm.

If no authentication mode or password is configured for an IP FPM instance on a DCP, the authentication mode and password configured for the DCP takes effect. If the authentication mode and password are configured in both the DCP view and IP FPM instance view, the configuration in the IP FPM instance view takes effect.

Example

Configure the authentication mode and password for an IP FPM instance.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] authentication-mode hmac-sha256 key-id 1 cipher Huawei-123
```

Related Topics

21.4.17 instance (IPFPM-DCP view)

21.4.2 authentication-mode (IPFPM-MCP view)

21.4.4 color-flag

Function

The **color-flag** command configures color bits.

The **undo color-flag** command restores the default color bits.

By default, the sixth bit in the ToS field of the IPv4 packet header is used as the loss color bit; the seventh bit in the ToS field of the IPv4 packet header is used as the delay color bit; Bit 0 in the Flags field of the IPv4 packet header is used as the multicast color bit. Using the default configurations is recommended.

Format

color-flag loss-measure { **tos-bit** *tos-bit* | **flags-bit0** } **delay-measure** { **tos-bit** *tos-bit* | **flags-bit0** }

undo color-flag

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
loss-measure	Indicates IP Flow Performance Measurement (IP FPM) packet loss measurement.	-
tos-bit *tos-bit*	Specifies a bit from the third to seventh bits in the ToS field of the IPv4 packet header as a color bit.	The value is an integer ranging from 3 to 7.
flags-bit0	Specifies Bit 0 in the Flags field of the IPv4 packet header as a color bit.	-
delay-measure	Indicates IP FPM delay measurement.	-

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before using IP FPM to measure network performance, run the **color-flag** command to specify a bit as a color bit based on network planning.

Precautions

All DCPs associated with an MCP must have the same multicast color bit configured.

The loss, delay, and multicast color bits cannot use the same bit, and the bits used for loss, and delay must not have been used in other measurement tasks.

Example

Configure IP FPM color bits.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] color-flag loss-measure tos-bit 3 delay-measure tos-bit 4
```

Related Topics

21.4.25 nqa ipfpm dcp

 Copyright © Huawei Technologies Co., Ltd.

21.4.5 dcp

Function

The **dcp** command specifies a Data Collecting Point (DCP) ID for an IP Flow Performance Measurement (IP FPM) instance on a MCP.

The **undo dcp** command deletes a DCP ID from an IP FPM instance on an MCP.

By default, no DCP ID is specified for an IP FPM instance on an MCP.

Format

dcp *dcp-id*

undo dcp [*dcp-id*]

Parameters

Parameter	Description	Value
dcp-id	Specifies the DCP ID of an IP FPM instance on an MCP. **NOTE** If *dcp-id* is not specified, the **undo dcp** command deletes all DCP IDs from a specified IP FPM instance on an MCP.	This value is in dotted decimal notation.

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IP FPM instance contains one or more DCPs. To specify DCP IDs for an IP FPM instance after it is created on an MCP, run the **dcp** command so that the MCP can determine whether the statistics are reported from authenticated DCPs.

Prerequisites

The **instance** command has been run to configure an IP FPM instance on an MCP.

Precautions

The DCP ID specified for an IP FPM instance on an MCP must be the same as that configured in the **dcp id** command on a DCP.

Copyright © Huawei Technologies Co., Ltd.

Example

Specify a DCP ID for IP FPM instance 1 on an MCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
[Huawei-nqa-ipfpm-mcp] instance 1
[Huawei-nqa-ipfpm-mcp-instance-1] dcp 10.1.1.1
```

Related Topics

21.4.26 nqa ipfpm mcp

21.4.16 instance (IPFPM-MCP view)

21.4.6 dcp id

Function

The **dcp id** command configures a DCP ID.

The **undo dcp id** command deletes a DCP ID.

By default, no DCP ID is configured.

Format

dcp id *dcp-id*

undo dcp id

Parameters

Parameter	Description	Value
dcp-id	ID of a DCP in the IP Flow Performance Measurement (IP FPM) model. Using the Router ID of a device that is configured as a DCP as its DCP ID is recommended.	This value is in dotted decimal notation.

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow communication between an MCP and a DCP, run the **dcp id** command to configure a DCP ID. After the DCP receives the statistics for an IP FPM instance from TLPs, the DCP encapsulates the statistics and the DCP ID to packets and

Copyright © Huawei Technologies Co., Ltd.

sends the packets with the DCP ID as the source IP address. After the MCP receives the packets, it compares the DCP ID carried in the packets with that configured in the **dcp** command run on itself.

- If the two DCP IDs are the same, the MCP accepts the packets and summarizes and calculates the statistics.
- If the two DCP IDs are different, the MCP considers the packets invalid and discards them.

Precautions

The DCP ID configured in an IP FPM instance must be the same as that specified in the **dcp** command run on an MCP. Otherwise, the MCP associated with this DCP cannot process the statistics reported by the DCP.

Example

Configure a DCP ID.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] dcp id 10.1.1.1
```

Related Topics

21.4.25 nqa ipfpm dcp

21.4.23 mcp id

21.4.5 dcp

21.4.7 delay-measure enable two-way

Function

The **delay-measure enable two-way** command enables on-demand two-way delay measurement for an IP FPM instance.

The **undo delay-measure enable two-way** command disables on-demand two-way delay measurement for an IP FPM instance.

By default, on-demand two-way delay measurement of an IP FPM instance is disabled.

Format

delay-measure enable two-way tlp *tlp-id1* [*tlp-id2*] [**continual** | **time-range** { **5** | **10** | **15** | **30** }]

undo delay-measure enable two-way

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
tlp *tlp-id1*	Specifies the TLP in-point for on-demand two-way delay measurement.	The value is an integer ranging from 1 to 16777215.
tlp-id2	Specifies the TLP out-point for on-demand two-way delay measurement. **NOTE** Currently, delay measurement is enabled by default for TLP out-points on the AR. Therefore, when enabling delay measurement, you must specify *tlp-id1*. *tlp-id2* can be specified as needed.	The value is an integer ranging from 1 to 16777215.
continual	Enables the continuous packet loss measurement function.	-
time-range { **5** | **10** | **15** | **30** }	Specifies the statistical period for on-demand two-way delay measurement. The value is an integer that can be 5, 10, 15, or 30, in minutes. The default value is 10 min.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IP FPM performance statistics serve as a reliable reference for assessing IP network performance and therefore are useful for fault diagnosis and service statistics. To monitor two-way delay performance in a specified period or diagnose network faults and locate faulty nodes when network performance deteriorates, run the **delay-measure enable two-way** command.

Prerequisites

An IP FPM model has been established, including configuring a DCP and MCP, binding a TLP to a physical interface, and creating a target flow and IP FPM instance.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Before implementing two-way delay measurement, ensure that the target flow in the IP FPM instance is bidirectional.

After a device restart, on-demand two-way delay measurement does not take effect any more.

After a master/slave main control board switchover, the measurement can be properly performed only when clock synchronization is complete. Clock synchronization takes a long time. Therefore, you are advised to reconfigure on-demand two-way delay measurement.

Example

Enable on-demand two-way delay measurement for an IP FPM instance.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] tlp 100 in-point ingress
[Huawei-nqa-ipfpm-dcp-instance-1] tlp 200 out-point egress
[Huawei-nqa-ipfpm-dcp-instance-1] delay-measure enable two-way tlp 100 200 time-range 15
```

Enable proactive two-way delay measurement for an IP FPM instance.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] tlp 100 in-point ingress
[Huawei-nqa-ipfpm-dcp-instance-1] tlp 200 out-point egress
[Huawei-nqa-ipfpm-dcp-instance-1] delay-measure enable two-way tlp 100 200 continual
```

Related Topics

21.4.25 nqa ipfpm dcp

21.4.17 instance (IPFPM-DCP view)

21.4.8 description (IPFPM-DCP instance view)

Function

The **description** command configures the description for an IP FPM instance.

The **undo description** command deletes the description of an IP FPM instance.

By default, no description is configured for an IP FPM instance.

Format

description *text*

undo description

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
text	Specifies the description of an IP FPM instance.	The value is a string of 1 to 64 case-sensitive characters, spaces supported.

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To help understand the services monitored by an IP FPM instance and the functions of the instance, run the **description** command to configure the description that shows detailed functions of the instance.

An IP FPM instance is identified by an integer ID, and therefore its functions are not easy to understand. Configuring the description for an IP FPM instance is recommended in the following situations:

- Many IP FPM instances are configured, and their functions cannot be clearly identified.
- An IP FPM instance is used at a long interval, and its function may be left forgotten.

Precautions

If an IP FPM instance is configured but does not have a description, it may be misused.

Example

Configure the description for IP FPM instance 1.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] description NanJinToHeFei
```

Related Topics

21.4.9 description (IPFPM-MCP instance view)

Copyright © Huawei Technologies Co., Ltd.

21.4.9 description (IPFPM-MCP instance view)

Function

The **description** command configures the description for an IP FPM instance.

The **undo description** command deletes the description of an IP FPM instance.

By default, no description is configured for an IP FPM instance.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of an IP FPM instance.	The value is a string of 1 to 64 case-sensitive characters, spaces supported.

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To help understand the services monitored by an IP FPM instance and the functions of the instance, run the **description** command to configure the description that shows detailed functions of the instance.

An IP FPM instance is identified by an integer ID, and therefore its functions are not easy to understand. Configuring the description for an IP FPM instance is recommended in the following situations:

- Many IP FPM instances are configured, and their functions cannot be clearly identified.
- An IP FPM instance is used at a long interval, and its function may be left forgotten.

Precautions

If an IP FPM instance is configured but does not have a description, it may be misused.

Copyright © Huawei Technologies Co., Ltd.

Example

Configure the description for IP FPM instance 1.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
[Huawei-nqa-ipfpm-mcp] instance 1
[Huawei-nqa-ipfpm-mcp-instance-1] description NanJinToHeFei
```

Related Topics

21.4.8 description (IPFPM-DCP instance view)

21.4.10 display ipfpm dcp

Function

The **display ipfpm dcp** command displays DCP configurations.

Format

display ipfpm dcp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check whether DCP configurations are correct, run the **display ipfpm dcp** command.

Example

Display DCP configurations.

```
<Huawei> display ipfpm dcp
Specification Information(Main Board):
 Max Instance Number                  :521
 Max 10s Instance Number              :521
 Max TLP Number                       :521
 Max TLP Number Per Instance          :8

Configuration Information:
 DCP ID                          : --
 Loss-measure Flag               : tos-bit6(default)
 Delay-measure Flag              : tos-bit7(default)
 Authentication Mode             : hmac-sha256
 Test Instances MCP ID           : --
```


Copyright © Huawei Technologies Co., Ltd.

```
Test Instances MCP Port          : 65030(default)
Current Instance Number          : 1
```

Table 21-26 Description of the **display ipfpm dcp** command output

Item	Description
Specification Information(Main Board)	Specifications for the main control board
Max Instance Number	Maximum number of IP FPM instances supported by the main control board
Max 10s Instance Number	Maximum number of IP FPM instances with the period of 10 seconds supported by the main control board
Max TLP Number	Maximum number of TLPs supported by the main control board
Max TLP Number Per Instance	Maximum number of TLPs supported by each IP FPM instance on the main control board
Configuration Information	DCP configurations
DCP ID	Data Collecting Point ID
Loss-measure Flag	Packet loss color bit: • tos-bit3: third bit in the ToS field of the IPv4 packet header • tos-bit4: fourth bit in the ToS field of the IPv4 packet header • tos-bit5: fifth bit in the ToS field of the IPv4 packet header • tos-bit6: sixth bit in the ToS field of the IPv4 packet header • tos-bit7: seventh bit in the ToS field of the IPv4 packet header • flag-bit0: Bit 0 in the Flags field of the IPv4 packet header

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Delay-measure Flag	Delay color bit: • tos-bit3: third bit in the ToS field of the IPv4 packet header • tos-bit4: fourth bit in the ToS field of the IPv4 packet header • tos-bit5: fifth bit in the ToS field of the IPv4 packet header • tos-bit6: sixth bit in the ToS field of the IPv4 packet header • tos-bit7: seventh bit in the ToS field of the IPv4 packet header • flag-bit0: Bit 0 in the Flags field of the IPv4 packet header
Authentication Mode	Authentication mode for the DCP: • hmac-sha256: HMAC-SHA256 authentication • --: non-authentication
Test Instances MCP ID	Measurement Control Point ID in the IP FPM instance
Test Instances MCP Port	User Datagram Protocol port number used by the DCP to communicate with the MCP in the IP FPM instance
Current Instance Number	Number of IP FPM instances

Related Topics

21.4.11 display ipfpm mcp

21.4.11 display ipfpm mcp

Function

The **display ipfpm mcp** command displays MCP configurations.

Format

display ipfpm mcp

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check whether MCP configurations are correct, run the **display ipfpm mcp** command.

Example

Display MCP configurations.

```
<Huawei> display ipfpm mcp
Specification Information:
 Max Instance Number                :128
 Max DCP Number Per Instance        :128

Configuration Information:
 MCP ID                             :--
 Status                             :Active
 Protocol Port                      :65030(default)
 Current Instance Number            :2
```

Table 21-27 Description of the **display ipfpm mcp** command output

Item	Description
Specification Information	Specifications for the MCP
Max Instance Number	Maximum number of IP FPM instances supported by the MCP
Max DCP Number Per Instance	Maximum number of DCPs supported by each IP FPM instance on the MCP
Configuration Information	MCP configurations
MCP ID	Measurement Control Point ID
Status	MCP status: • Active • Deleting
Protocol Port	UDP port number used for the MCP to communicate with DCPs
Total Instances	Number of IP FPM instances

Related Topics

21.4.10 display ipfpm dcp

Copyright © Huawei Technologies Co., Ltd.

21.4.12 display ipfpm instance application

Function

The **display ipfpm instance application** command displays the relationship between IP FPM instances and applications.

Format

display ipfpm instance application

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view the relationship between IP FPM instances and applications.

Precautions

Before running the **display ipfpm instance application** command, you need to run the **flow application** *application-name* command first to configure application matching information of the target flow.

Example

Display the relationship between IP FPM instances and applications.

```
<Huawei> display ipfpm instance application
-------------------------------------------------------------------------------
 Index          InstanceId          APPid          APPName
-------------------------------------------------------------------------------
 1              1                   3559           DBank
 2              2                   101            QQHuaXia
 3              3                   3560           DBankSync
-------------------------------------------------------------------------------
```

Table 21-28 Description of the **display ipfpm instance application** command output

Item	Description
Index	Index of a test record.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
InstanceId	ID of an instance.
APPid	ID of an application.
APPName	Name of an application.

Related Topics

21.4.15 flow (IPFPM-DCP instance view)

21.4.13 display ipfpm statistic-type

Function

The **display ipfpm statistic-type** command displays performance statistics for an IP FPM instance.

Format

display ipfpm statistic-type { **loss** | **twoway-delay** } **instance** *instance-id*

Parameters

Parameter	Description	Value
loss	Displays packet loss statistics.	-
twoway-delay	Displays two-way delay statistics.	-
instance *instance-id*	Specifies an IP FPM instance ID.	The value is an integer ranging from 1 to 16777214.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check the number of discarded packets, packet loss rate, one-way and two-way delay statistics, and jitter of an IP FPM instance, run the **display ipfpm statistic-**

Copyright © Huawei Technologies Co., Ltd.

type command. To locate and diagnose network faults when network performance deteriorates, run the **display ipfpm statistic-type** command with **ach** configured to check statistics for a specified ACH.

Precautions

This command is valid only on MCPs.

The first statistics collected may not be accurate, therefore, using subsequent statistics as a reference for network performance is recommended.

The precision of NTP clock synchronization is different from that of IP FPM measurement. As a result, the data reported by IP FPM may be inaccurate and a negative number may be generated.

Example

Display the packet loss statistics for IP FPM instance 1 on an MCP.

```
<Huawei> display ipfpm statistic-type loss instance 1
Latest loss statistics of forward flow:
Unit: p - packet, b - byte
-------------------------------------------------------------------------------------
 Period          Loss(p)          LossRatio(p)  Loss(b)          LossRatio(b)
-------------------------------------------------------------------------------------
 136118757         20               20.000000% 2000               20.000000%
 136118756         20               20.000000% 2000               20.000000%
 136118755         20               20.000000% 2000               20.000000%
 136118753         20               20.000000% 2000               20.000000%
 136118752         20               20.000000% 2000               20.000000%
 136118751         20               20.000000% 2000               20.000000%
 136118750         20               20.000000% 2000               20.000000%
 136118749         20               20.000000% 2000               20.000000%
 136118748         20               20.000000% 2000               20.000000%
 136118747         20               20.000000% 2000               20.000000%
 136118746         20               20.000000% 2000               20.000000%
 136118745         20               20.000000% 2000               20.000000%

Latest loss statistics of backward flow:
Unit: p - packet, b - byte
-------------------------------------------------------------------------------------
 Period          Loss(p)          LossRatio(p)  Loss(b)          LossRatio(b)
-------------------------------------------------------------------------------------
 136118757         20               20.000000% 2000               20.000000%
 136118756         20               20.000000% 2000               20.000000%
 136118755         20               20.000000% 2000               20.000000%
 136118753         20               20.000000% 2000               20.000000%
 136118752         20               20.000000% 2000               20.000000%
 136118751         20               20.000000% 2000               20.000000%
 136118750         20               20.000000% 2000               20.000000%
 136118749         20               20.000000% 2000               20.000000%
 136118748         20               20.000000% 2000               20.000000%
 136118747         20               20.000000% 2000               20.000000%
 136118746         20               20.000000% 2000               20.000000%
 136118745         20               20.000000% 2000               20.000000%
```

Display the two-way delay statistics for IP FPM instance 1 on an MCP.

```
<Huawei> display ipfpm statistic-type twoway-delay instance 1
Latest two-way delay statistics:
-------------------------------------------------
 Period          Delay(usec) Delay
                             Variation(usec)
-------------------------------------------------
 136118757         800         0
 136118756         800         0
```

 Copyright © Huawei Technologies Co., Ltd.

```
136118755          800         0
136118753          800         0
136118752          800         0
136118751          800         0
136118750          800         0
136118749          800         0
136118748          800         0
136118747          800         0
136118746          800         0
136118745          800         0

Latest one-way delay statistics of bidirectional flow:
-------------------------------------------------------------------------------
Period          Forward      ForwardDelay    Backward     BackwardDelay
                Delay(usec)  Variation(usec) Delay(usec)  Variation(usec)
-------------------------------------------------------------------------------
136118757          400         0               400          0
136118756          400         0               400          0
136118755          400         0               400          0
136118753          400         0               400          0
136118752          400         0               400          0
136118751          400         0               400          0
136118750          400         0               400          0
136118749          400         0               400          0
136118748          400         0               400          0
136118747          400         0               400          0
136118746          400         0               400          0
136118745          400         0               400          0
```

Table 21-29 Description of the **display ipfpm statistic-type** command output

Item	Description
Period	Statistical period ID
Loss(p)	Number of discarded packets
LossRatio(p)	Packet loss rate
Loss(b)	Number of discarded bytes
LossRatio(b)	Byte loss rate
Delay(usec)	Delay, in microseconds
DelayVariation(usec)	Jitter, in microseconds
ForwardDelay(usec)	Delay for the forward delay, in microseconds
ForwardDelayVariation(usec)	Jitter for the forward delay, in microseconds
BackwardDelay(usec)	Delay for the backward delay, in microseconds
BackwardDelayVariation(usec)	Jitter for the backward delay, in microseconds

Copyright © Huawei Technologies Co., Ltd.

21.4.14 display snmp-agent trap feature-name ipfpm all

Function

The **display snmp-agent trap feature-name ipfpm all** command displays configurations of all alarm functions of the IP FPM module.

Format

display snmp-agent trap feature-name ipfpm all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check whether the alarm functions of the IP FPM module are enabled, run the **display snmp-agent trap feature-name ipfpm all** command.

Example

Display configurations of all alarm functions of the IP FPM module.

```
<Huawei> display snmp-agent trap feature-name ipfpm all
------------------------------------------------------------------------------
Feature name: IPFPM
Trap number : 8
------------------------------------------------------------------------------
Trap name                     Default switch status   Current switch status
hwIpfpmLossRatioExceed        off                     off
hwIpfpmLossRatioRecovery      off                     off
hwIpfpmOneDelayExceed         off                     off
hwIpfpmOneDelayRecovery       off                     off
hwIpfpmTwoDelayExceed         off                     off
hwIpfpmTwoDelayRecovery       off                     off
hwIpfpmTlpExceed              off                     off
hwIpfpmTlpRecovery            off                     off
```

Table 21-30 Description of the **display snmp-agent trap feature-name ipfpm all** command output

Item	Description
Feature name	Name of the module to which the alarms are related
Trap number	Number of alarms

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trap name	Names of alarms related to the IP FPM module: • hwIpfpmLossRatioExceed: packet loss alarm • hwIpfpmLossRatioRecovery: packet loss clear alarm • hwIpfpmOneDelayExceed: one-way delay alarm • hwIpfpmOneDelayRecovery: one-way delay clear alarm • hwIpfpmTwoDelayExceed: two-way delay alarm • hwIpfpmTwoDelayRecovery: two-way delay clear alarm • hwIpfpmTlpExceed: TLPs threshold-crossing alarm • hwIpfpmTlpRecovery: TLPs threshold-crossing clear alarm
Default switch status	Default alarm status • on: The alarm function is enabled. • off: The alarm function is disabled.
Current switch status	Current alarm status • on: The alarm function is enabled. • off: The alarm function is disabled.

Related Topics

21.4.28 snmp-agent trap enable feature-name ipfpm

21.4.15 flow (IPFPM-DCP instance view)

Function

The **flow** command configures the target flow characteristics for an IP FPM instance.

The **undo flow** command deletes the target flow characteristics of an IP FPM instance.

By default, no characteristics are configured for the target flow of an IP FPM instance.

Format

flow forward { **dscp** *dscp-value* | **source** *src-ip-address* [*src-mask-length*] | **destination** *dest-ip-address* [*dest-mask-length*] | **protocol** { { **tcp** | **udp** } { **source-port** *src-port-number1* [**to** *src-port-number2*] | **destination-port** *dest-port-number1* [**to** *dest-port-number2*] } * | *protocol-number* } } *

flow backward { **dscp** *dscp-value* | **source** *src-ip-address* [*src-mask-length*] | **destination** *dest-ip-address* [*dest-mask-length*] | **protocol** { { **tcp** | **udp** }

 Copyright © Huawei Technologies Co., Ltd.

{ **source-port** *src-port-number1* [**to** *src-port-number2*] | **destination-port** *dest-port-number1* [**to** *dest-port-number2*] } * | *protocol-number* } } *

flow bidirectional { **dscp** *dscp-value* | **source** *src-ip-address* [*src-mask-length*] | **destination** *dest-ip-address* [*dest-mask-length*] | **protocol** { { **tcp** | **udp** } { **source-port** *src-port-number1* [**to** *src-port-number2*] | **destination-port** *dest-port-number1* [**to** *dest-port-number2*] } * | *protocol-number* } } *

flow application *application-name*

undo flow { **forward** | **backward** | **bidirectional** | **application** }

Parameters

Parameter	Description	Value
forward	Indicates the forward target flow.	-
backward	Indicates the backward target flow.	-
bidirectional	Indicates the symmetrical bidirectional target flow. **NOTE** If the target flow is symmetrical bidirectional, set *src-ip-address* to specify a source IP address and *dest-ip-address* to specify a destination IP address for the target flow.	-
application	Specifies the application protocol of the target flow.	-
dscp *dscp-value*	Specifies the DSCP value of the target flow.	The value is an integer ranging from 0 to 63.
source *src-ip-address*	Specifies the source IP address of the target flow.	This value is in dotted decimal notation.
src-mask-length	Specifies the mask length of the source IP address of the target flow.	The value is an integer ranging from 1 to 32.
destination *dest-ip-address*	Specifies the destination IP address of the target flow.	This value is in dotted decimal notation.
dest-mask-length	Specifies the mask length of the destination IP address of the target flow.	The value is an integer ranging from 1 to 32.
protocol	Indicates the protocol type of the target flow.	-
tcp	Indicates that the protocol type of the target flow is TCP.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
udp	Indicates that the protocol type of the target flow is UDP.	-
source-port *src-port-number1*	Specifies the start source port number of the target flow.	The value is an integer ranging from 1 to 65535.
src-port-number2	Specifies the end source port number of the target flow.	The value is an integer ranging from 1 to 65535. *src-port-number2* must be greater than *src-port-number1*.
destination-port *dest-port-number1*	Specifies the start destination port number of the target flow.	The value is an integer ranging from 1 to 65535.
dest-port-number2	Specifies the end destination port number of the target flow.	The value is an integer ranging from 1 to 65535. *dest-port-number2* must be greater than *dest-port-number1*.
protocol-number	Indicates the protocol number of the target flow.	The value is an integer ranging from 1 to 5, 7 to 16, or 18 to 255. **NOTE** The value 6 indicates TCP, and the value 17 indicates UDP.
application-name	Specifies the name of the application protocol.	The value is a string of characters without spaces. The value depends on application protocols in the signature database.

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

One or more fields in IP headers can be specified to identify target flows. The field can be the source IP address or prefix, destination IP address or prefix, protocol type, source port number, destination port number, or ToS. The more fields specified, the more accurately flows can be identified. Specifying as many fields as possible is recommended to maximize the measurement accuracy.

Copyright © Huawei Technologies Co., Ltd.

To define target flows and ensure measurement accuracy, run the **flow** command to configure target flow characteristics.

Configuration Impact

An IP FPM instance can have only one target flow configured, either unidirectional or bidirectional. A bidirectional target flow is logically two unidirectional flows in opposite directions.

- If the target flow in an IP FPM instance is bidirectional, two situations are available:
  - If the bidirectional target flow is symmetrical, you can specify **bidirectional** to configure the bidirectional target flow characteristics. By default, the characteristics specified are used for the forward flow, and the reverse of those are used for the backward flow. Specifically, the source and destination IP addresses and port numbers specified for the forward flow are used respectively as the destination and source IP addresses and port numbers for the backward flow.
  - If the bidirectional target flow is asymmetrical, you must configure **forward** and **backward** in two command instances to configure the forward and backward flow characteristics.

Precautions

Target flows in different IP FPM instances cannot have the same characteristics. The forward and backward target flows in an IP FPM instance cannot have the same characteristics neither.

To make the application protocol of the target flow configured for a specified **application** in an IP FPM instance take effect, you need to specify **bidirectional**, **forward**, or **backward** to configure any flow characteristic of bidirectional target flow, forward target flow, and backward target flow. In addition, you need to run the **sa application-statistic enable** command on the interface to enable SAC before using the IP FPM function.

Example

Configure the target flow characteristics for IP FPM instance 1.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] flow bidirectional source 1.1.1.1 destination 2.2.2.2
```

Related Topics

21.4.25 nqa ipfpm dcp

21.4.17 instance (IPFPM-DCP view)

21.4.16 instance (IPFPM-MCP view)

Function

The **instance** command creates an IP FPM instance on a Measurement Control Point (MCP) and displays the instance view.

The **undo instance** command deletes an IP FPM instance of an MCP.

Copyright © Huawei Technologies Co., Ltd.

By default, no IP FPM instance is created on MCPs.

Format

instance *instance-id*

undo instance *instance-id*

Parameters

Parameter	Description	Value
instance-id	Specifies the ID of an IP FPM instance.	The value is an integer ranging from 1 to 8355838.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement IP FPM performance statistics on a specified service flow, run the **instance** command to create an IP FPM instance. Each IP FPM instance is composed of a target flow, TLPs, and a statistical period.

Precautions

The IP FPM instance ID must be unique on an MCP and all its associated DCPs.

An MCP and all its associated DCPs must have the same IP FPM instance configured. Otherwise, statistics collection does not take effect.

Example

Create an IP FPM instance on an MCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
[Huawei-nqa-ipfpm-mcp] instance 1
```

Related Topics

21.4.26 nqa ipfpm mcp

21.4.9 description (IPFPM-MCP instance view)

21.4.17 instance (IPFPM-DCP view)

Copyright © Huawei Technologies Co., Ltd.

21.4.17 instance (IPFPM-DCP view)

Function

The **instance** command creates an IP FPM instance on a DCP and displays the instance view.

The **undo instance** command deletes an IP FPM instance of a DCP.

By default, no IP FPM instance is created on DCPs.

Format

instance *instance-id*

undo instance *instance-id*

Parameters

Parameter	Description	Value
instance-id	Specifies the ID of an IP FPM instance.	The value is an integer ranging from 1 to 8355838.

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement IP FPM performance statistics on a specified service flow, run the **instance** command to create an IP FPM instance. Each IP FPM instance is composed of a target flow, TLPs, and a statistical period.

Follow-up Procedure

Run the following commands to configure parameters for the configured IP FPM instance.

- Run the **flow** command to configure target flow characteristics.
- Run the **tlp** command to configure a TLP.
- Run the **interval** command to configure the statistical period.

Precautions

The IP FPM instance ID must be unique on an MCP and all its associated DCPs.

An MCP and all its associated DCPs must have the same IP FPM instance configured. Otherwise, statistics collection does not take effect.

Copyright © Huawei Technologies Co., Ltd.

Example

Create an IP FPM instance on a DCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
```

Related Topics

21.4.25 nqa ipfpm dcp
21.4.8 description (IPFPM-DCP instance view)
21.4.16 instance (IPFPM-MCP view)
21.4.15 flow (IPFPM-DCP instance view)
21.4.29 tlp
21.4.18 interval

21.4.18 interval

Function

The **interval** command configures the statistical period for an IP FPM instance.

The **undo interval** command restores the default statistical period of an IP FPM instance.

By default, the statistical period is 10s.

Format

interval { **10** | **60** | **600** }

undo interval

Parameters

Parameter	Description	Value
10	Specifies the statistical period for an IP FPM instance as 10s.	-
60	Specifies the statistical period for an IP FPM instance as 60s.	-
600	Specifies the statistical period for an IP FPM instance as 600s.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To implement IP FPM performance statistics and ensure measurement accuracy, run the **interval** command to configure a statistical period based on the clock offset, maximum transmission delay, and system performance.

The statistical period of an IP FPM instance is a period of time from when TLPs measure the number of packets or bytes to when DCPs report the statistics to an MCP and the MCP calculates the measurement result.

The shorter the statistical period, the more frequent DCPs report the statistics to the MCP, and the more statistics the DCPs and MCP will process. Therefore, the statistical period change will affect the system performance of the DCPs and MCP.

Configuration Impact

If the statistical period of an IP FPM instance is changed, it must be changed for all DCPs of this IP FPM instance. Otherwise, statistics collection does not take effect.

Precautions

To ensure statistics accuracy, before you change the statistical period of an IP FPM instance, disabling packet loss or delay measurement in the instance view is recommended.

Example

Configure the statistical period for IP FPM instance 1 as 60s.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] interval 60
```

Related Topics

21.4.25 nqa ipfpm dcp

21.4.17 instance (IPFPM-DCP view)

21.4.15 flow (IPFPM-DCP instance view)

21.4.7 delay-measure enable two-way

21.4.19 ipfpm tlp (layer 3 interface)

Function

The **ipfpm tlp** command binds a Target Logical Port (TLP) to an interface.

The **undo ipfpm tlp** command unbinds a TLP from an interface.

By default, a TLP is not bound to any interface.

Format

ipfpm tlp *tlp-id*

Copyright © Huawei Technologies Co., Ltd.

undo ipfpm tlp { *tlp-id* | **all** }

Parameters

Parameter	Description	Value
tlp-id	Specifies a TLP ID.	The value is an integer ranging from 1 to 16777215.
all	Unbinds TLP from all interfaces in the IP FPM statistical system.	-

Views

interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before implementing IP FPM performance statistics, ensure that TLPs are bound to interfaces.

Precautions

A TLP can be bound to only one interface on the DCPs associated with an MCP.

Example

Bind the interface GigabitEthernet0/0/0 to TLP 100.

```
<Huawei> system-view
[Huawei] interface Gigabitethernet0/0/0
[Huawei-GigabitEthernet0/0/0] ipfpm tlp 100
```

Related Topics

21.4.29 tlp

21.4.20 loss-measure enable

Function

The **loss-measure enable** command enables on-demand packet loss measurement for an IP FPM instance.

The **undo loss-measure enable** command disables on-demand packet loss measurement for an IP FPM instance.

By default, on-demand packet loss measurement is disabled for an IP FPM instance.

Copyright © Huawei Technologies Co., Ltd.

Format

loss-measure enable [**continual** | **time-range** { **5** | **10** | **15** | **30** }]

undo loss-measure enable [**continual** | **time-range** { **5** | **10** | **15** | **30** }]

Parameters

Parameter	Description	Value
continual	Enables the continuous packet loss measurement function.	-
time-range { **5** | **10** | **15** | **30** }	Specifies the statistical period for on-demand packet loss measurement. The value is an integer that can be 5, 10, 15, or 30, in minutes. The default value is 10min.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IP FPM performance statistics serve as a reliable reference for assessing IP network performance and therefore are useful for fault diagnosis and service statistics. To monitor on-demand packet loss performance in a specified period or diagnose network faults and locate faulty nodes when network performance deteriorates, run the **loss-measure enable** command.

Prerequisites

An IP FPM model has been established, including configuring a DCP and MCP, binding a TLP to a physical interface, and creating a target flow and IP FPM instance.

Precautions

After a device restart, on-demand packet loss measurement does not take effect any more.

After a master/slave main control board switchover, the measurement can be properly performed only when clock synchronization is complete. Clock synchronization takes a long time. Therefore, you are advised to reconfigure on-demand packet loss measurement.

On-demand packet loss measurement cannot be enabled together with continuous packet loss measurement. If the continuous packet loss measurement

 Copyright © Huawei Technologies Co., Ltd.

function is enabled first, on-demand packet loss measurement can be enabled successfully only when the **undo loss-measure enable continual** command is run.

Example

Enable on-demand packet loss measurement for an IP FPM instance.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] loss-measure enable time-range 30
```

Enable proactive packet loss measurement for an IP FPM instance.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] loss-measure enable continual
```

Related Topics

21.4.25 nqa ipfpm dcp

21.4.17 instance (IPFPM-DCP view)

21.4.21 mcp (IPFPM-DCP instance view)

Function

The **mcp** command specifies a Measurement Control Point (MCP) ID for an IP Flow Performance Measurement (IP FPM) instance on a Data Collecting Point (DCP).

The **undo mcp** command deletes the MCP ID of an IP FPM instance on a DCP.

By default, no MCP ID is specified for an IP FPM instance on a DCP.

Format

mcp *mcp-id* [**port** *port-number*] [**vpn-instance** *vpn-instance-name* | **net-manager-vpn**]

undo mcp

Parameters

Parameter	Description	Value
mcp-id	Specifies an MCP ID for an IP FPM instance on a DCP. Using the Router ID of a device that is configured as an MCP as its MCP ID is recommended.	This value is in dotted decimal notation.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
port *port-number*	Specifies a UDP port number for a DCP to communicate with an MCP.	The value is an integer ranging from 1024 to 65535. The default value is 65030 and is recommended.
vpn-instance *vpn-instance-name*	Specifies a VPN instance for a DCP to communicate with an MCP.	The name is a string of 1 to 31 case-sensitive characters without any spaces.
net-manager-vpn	Specifies a management VPN for a DCP to communicate with an MCP.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow a DCP in an IP FPM instance to report the statistics collected by TLPs to an MCP, run the **mcp** command to specify the MCP ID for the DCP in this instance.

Prerequisites

The **instance** command has been run to configure an IP FPM instance.

NOTE

The VPN instance has been created on the DCP before you configure **vpn-instance** *vpn-instance-name* or **net-manager-vpn** to allow the DCP to report the statistics to the MCP through the specified VPN or management VPN.

Implementation

After receiving the statistics for an IP FPM instance from TLPs, a DCP encapsulates the statistics and the MCP ID in the IP FPM instance to packets and sends the packets to the destination IP address identified by the MCP ID. After the MCP receives the packets, it compares the MCP ID carried in the packets with that configured in the **mcp id** command run on itself.

- If the two MCP IDs are the same, the MCP accepts the packets and summarizes and calculates the statistics.
- If the two MCP IDs are different, the MCP considers the packets invalid and discards them.

Copyright © Huawei Technologies Co., Ltd.

Precautions

The MCP ID must be an IP address reachable to the DCPs. The MCP ID specified for an IP FPM instance on a DCP must be the same as that specified in the **mcp id** command run on the MCP associated with this DCP.

The UDP port number configured on the DCP must be the same as that configured in the **protocol udp port** command run on the MCP associated with this DCP. Otherwise, the DCP cannot report the statistics to the MCP.

Example

Specify the MCP ID for IP FPM instance 1 on a DCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] mcp 10.1.1.1
```

Specify the MCP ID for IP FPM instance 1 on a DCP and configure the DCP to send statistics to the MCP through the VPN instance **vpnforipfpm**.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] mcp 10.1.1.1 vpn-instance vpnforipfpm
```

21.4.22 mcp (IPFPM-DCP view)

Function

The **mcp** command specifies a MCP ID for all IP FPM instances on a DCP.

The **undo mcp** command deletes the MCP ID of all IP FPM instances on a DCP.

By default, no MCP ID is specified for IP FPM instances on a DCP.

Format

mcp *mcp-id* [**port** *port-number*] [**vpn-instance** *vpn-instance-name* | **net-manager-vpn**]

undo mcp

Parameters

Parameter	Description	Value
mcp-id	Specifies an MCP ID for all IP FPM instances on a DCP. Using the Router ID of a device that is configured as an MCP as its MCP ID is recommended.	This value is in dotted decimal notation.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
port *port-number*	Specifies a UDP port number for a DCP to communicate with an MCP.	The value is an integer ranging from 1024 to 65535. The default value is 65030 and is recommended.
vpn-instance *vpn-instance-name*	Specifies a VPN instance for a DCP to communicate with an MCP.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
net-manager-vpn	Specifies a management VPN for a DCP to communicate with an MCP.	-

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow a DCP in an IP FPM instance to report the statistics collected by TLPs to an MCP, run the **mcp** command to specify the MCP ID for all IP FPM instances on the DCP.

Prerequisites

The **nqa ipfpm dcp** command has been run to enable DCP globally.

NOTE

The VPN instance has been created on the DCP before you configure **vpn-instance** *vpn-instance-name* or **net-manager-vpn** to allow the DCP to report the statistics to the MCP through the specified VPN or management VPN.

Implementation

After receiving the statistics for all IP FPM instances from TLPs, a DCP encapsulates the statistics and the MCP ID in the IP FPM instances to packets and sends the packets to the destination IP address identified by the MCP ID. After the MCP receives the packets, it compares the MCP ID carried in the packets with that configured in the **mcp id** command run on itself.

- If the two MCP IDs are the same, the MCP accepts the packets and summarizes and calculates the statistics.

 Copyright © Huawei Technologies Co., Ltd.

- If the two MCP IDs are different, the MCP considers the packets invalid and discards them.

Precautions

The MCP ID must be an IP address reachable to DCPs. The MCP ID specified for all IP FPM instances on a DCP must be the same as that specified in the **mcp id** command run on the MCP associated with this DCP.

The UDP port number configured on the DCP must be the same as that configured in the **protocol udp port** command run on the MCP associated with this DCP. Otherwise, the DCP cannot report the statistics to the MCP.

If the **mcp** command has been run in the IP FPM instance view for some instances on a DCP and an MCP ID is specified for all IP FPM instances on the DCP, the MCP ID specified in the IP FPM instance view takes effect.

Example

Specify the MCP ID for all IP FPM instances on a DCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] mcp 10.1.1.1
```

Specify the MCP ID for IP FPM instance 1 on a DCP and configure the DCP to send statistics to the MCP through the VPN instance **vpnforipfpm**.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] mcp 10.1.1.1 vpn-instance vpnforipfpm
```

Related Topics

21.4.25 nqa ipfpm dcp
21.4.27 protocol udp port
21.4.23 mcp id

21.4.23 mcp id

Function

The **mcp id** command configures an MCP ID.

The **undo mcp id** command deletes an MCP ID.

By default, no MCP ID is configured.

Format

mcp id *mcp-id*

undo mcp id

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mcp-id	Specifies an MCP ID. Using the Router ID of a device that is configured as an MCP as its MCP ID is recommended.	This value is in dotted decimal notation.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow communication between an MCP and a DCP, run the **mcp id** command to configure an MCP ID. After the DCP receives the statistics for an IP FPM instance from TLPs, the DCP encapsulates the statistics and the MCP ID specified by the **mcp** command run in the IP FPM instance to packets and sends the packets to the destination IP address identified by the MCP ID. After the MCP receives the packets, it compares the MCP ID carried in the packets with that configured in the **mcp id** command run on itself.

- If the two MCP IDs are the same, the MCP accepts the packets and summarizes and calculates the statistics.
- If the two MCP IDs are different, the MCP considers the packets invalid and discards them.

Precautions

The MCP ID must be an IP address reachable to DCPs. The MCP ID configured on an MCP must be the same as that specified in the **mcp** command run in the IP FPM instance view of all DCPs associated with this MCP. If an MCP ID is changed on an MCP, it must be changed for all DCPs associated with this MCP in an IP FPM instance. Otherwise, the MCP cannot process the statistics reported by the DCPs.

Example

Configure an MCP ID.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
[Huawei-nqa-ipfpm-mcp] mcp id 10.1.1.1
```

21.4.24 measure disable (IPFPM-MCP instance view)

Copyright © Huawei Technologies Co., Ltd.

Function

The **measure disable** command disables IP FPM performance statistics collection of a specified instance on a MCP.

The **undo measure disable** and **measure enable** commands function the same to enable IP FPM performance statistics collection for a specified instance on an MCP.

By default, IP FPM performance statistics collection is enabled for instances on an MCP.

Format

measure disable

measure enable

undo measure disable

Parameters

None

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

When DCP configurations are being changed, the MCP may receive incorrect statistics from the DCP. To prevent this, run the **measure disable** command to disable IP FPM performance statistics collection of a specified instance on the MCP. After the DCP configuration change is complete, run the **undo measure disable** or **measure enable** command to enable IP FPM performance statistics collection for the specified instance on the MCP. This ensures accurate measurement.

Example

Disable IP FPM performance statistics collection of a specified instance on an MCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
[Huawei-nqa-ipfpm-mcp] instance 1
[Huawei-nqa-ipfpm-mcp-instance-1] measure disable
```

Related Topics

21.4.26 nqa ipfpm mcp

Copyright © Huawei Technologies Co., Ltd.

21.4.25 nqa ipfpm dcp

Function

The **nqa ipfpm dcp** command enables DCP globally and displays the IPFPM-DCP view.

The **undo nqa ipfpm dcp** command disables DCP globally.

By default, DCP is disabled globally.

Format

nqa ipfpm dcp

undo nqa ipfpm dcp

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable DCP globally so that IP FPM performance statistics can be implemented, run the **nqa ipfpm dcp** command. A DCP manages and controls TLPs, collects statistics generated by TLPs, and reports the statistics to an MCP.

Follow-up Procedure

Run the **dcp id** command to configure a DCP ID.

Precautions

DCP and MCP functionalities can be configured on the same device.

Example

Enable DCP globally and display the IPFPM-DCP view.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
```

Related Topics

21.4.6 dcp id

21.4.26 nqa ipfpm mcp

Copyright © Huawei Technologies Co., Ltd.

21.4.26 nqa ipfpm mcp

Function

The **nqa ipfpm mcp** command enables Measurement Control Point (MCP) globally and displays the IPFPM-MCP view.

The **undo nqa ipfpm mcp** command disables MCP globally.

By default, MCP is enabled globally.

Format

nqa ipfpm mcp

undo nqa ipfpm mcp

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable MCP globally so that IP FPM performance statistics can be implemented, run the **nqa ipfpm mcp** command. An MCP collects statistics reported by DCPs, summarizes and calculates the statistics, and reports measurement results to user terminals or the NMS.

Follow-up Procedure

Run the **mcp id** command to configure an MCP ID.

Precautions

MCP and DCP functionalities can be configured on the same device.

Example

Enable MCP globally and display the IPFPM-MCP view.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
```

Related Topics

21.4.23 mcp id

Copyright © Huawei Technologies Co., Ltd.

21.4.25 nqa ipfpm dcp

21.4.27 protocol udp port

Function

The **protocol udp port** command configures an User Datagram Protocol (UDP) port number for a MCP to communicate with DCPs.

The **undo protocol udp port** command restores the default UDP port number for an MCP to communicate with DCPs.

By default, an MCP uses UDP port 65030 to communicate with DCPs.

Format

protocol udp port *port-number*

undo protocol udp port

Parameters

Parameter	Description	Value
port-number	Specifies the UDP port number for an MCP to communicate with DCPs.	The value is an integer ranging from 1024 to 65535.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an MCP uses UDP port 65030 to communicate with DCPs. To change the default UDP port number for an MCP to communicate with DCPs, run the **protocol udp port** command.

Precautions

The UDP port number configured on an MCP must be the same as that specified in the **mcp** command run in the IP FPM instance view of all DCPs associated with this MCP. If a UDP port number is changed on an MCP, it must be changed for all DCPs associated with this MCP in an IP FPM instance. Otherwise, the MCP cannot process the statistics reported by the DCPs.

Copyright © Huawei Technologies Co., Ltd.

Example

Specify UDP port 1024 for an MCP to communicate with DCPs.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
[Huawei-nqa-ipfpm-mcp] protocol udp port 1024
```

Related Topics

21.4.23 mcp id

21.4.26 nqa ipfpm mcp

21.4.25 nqa ipfpm dcp

21.4.28 snmp-agent trap enable feature-name ipfpm

Function

The **snmp-agent trap enable feature-name ipfpm** command enables the alarm function for the IP FPM module.

The **undo snmp-agent trap enable feature-name ipfpm** command disables the alarm function of the IP FPM module.

By default, the alarm function of the IP FPM module is disabled.

Format

snmp-agent trap enable feature-name ipfpm [**trap-name** { **hwipfpmlossratioexceed** | **hwipfpmlossratiorecovery** | **hwipfpmonedelayexceed** | **hwipfpmonedelayrecovery** | **hwipfpmtwodelayexceed** | **hwipfpmtwodelayrecovery** | **hwipfpmtlpexceed** | **hwipfpmtlprecovery**}]

undo snmp-agent trap enable feature-name ipfpm [**trap-name** { **hwipfpmlossratioexceed** | **hwipfpmlossratiorecovery** | **hwipfpmonedelayexceed** | **hwipfpmonedelayrecovery** | **hwipfpmtwodelayexceed** | **hwipfpmtwodelayrecovery** | **hwipfpmtlpexceed** | **hwipfpmtlprecovery**}]

Parameters

Parameter	Description	Value
trap-name	Indicates the alarm function for a specific type of event.	-
hwipfpmlossratioexceed	Indicates the packet loss alarm function.	-
hwipfpmlossratiorecovery	Indicates the packet loss clear alarm function.	-
hwipfpmonedelayexceed	Indicates the one-way delay alarm.	-
hwipfpmonedelayrecovery	Indicates the one-way delay clear alarm.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwipfpmtwodelayexceed	Indicates the two-way delay alarm.	-
hwipfpmtwodelayrecovery	Indicates the two-way delay clear alarm.	-
hwipfpmtlpexceed	Indicates the TLPs threshold-crossing alarm.	-
hwipfpmtlprecovery	Indicates the TLPs threshold-crossing clear alarm.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow a device to use SNMP to report IP FPM alarms to the NMS, run the **snmp-agent trap enable feature-name ipfpm** command to enable the alarm function. SNMP is a widely used network management protocol that collects network communication statistics using agent software embedded in managed devices.

Precautions

If you do not configure **trap-name** in the **snmp-agent trap enable feature-name ipfpm** command, the command enables all alarm functions for the IP FPM module. If **trap-name** is configured, a specific alarm function is enabled.

Example

Enable the two-way delay alarm.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name ipfpm trap-name hwipfpmtwodelayexceed
```

Related Topics

21.4.14 display snmp-agent trap feature-name ipfpm all

21.4.29 tlp

Function

The **tlp** command configures a Target Logical Port (TLP) for an IP FPM instance and specifies the TLP role.

The **undo tlp** command deletes a TLP of an IP FPM instance.

By default, no TLP is configured for an IP FPM instance.

Copyright © Huawei Technologies Co., Ltd.

Format

tlp *tlp-id* { **in-point** | **out-point** } { **ingress** | **egress** }

undo tlp *tlp-id*

Parameters

Parameter	Description	Value
tlp-id	Specifies a TLP ID.	The value is an integer ranging from 1 to 16777215.
in-point	Specifies a TLP as an in-point. The system sets the measurement flags of target flows on an in-point.	-
ingress	Indicates the upstream target flow.	-
out-point	Specifies a TLP as an out-point. The system clears the measurement flags of target flows on an out-point.	-
egress	Indicates the downstream target flow.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To locate faults in IP FPM performance statistics scenarios, run the **tlp** command to configure TLPs in an IP FPM instance. TLPs are measurement points along the path of the target flow and compile and output the statistics. TLPs can be in-points, mid-points, or out-points.

Precautions

A TLP that functions as the in-point for the forward target flow is the out-point for the backward target flow. The TLP role specified in the **tlp** *tlp-id* { **in-point ingress** | **out-point egress** } command applies only to the forward target flow, and the reverse of the specified role is used for the backward target flow.

A TLP cannot function as both the in-point and out-point for the same unidirectional target flow.

Copyright © Huawei Technologies Co., Ltd.

Example

Configure a TLP for IP FPM instance 1 and specify the TLP role.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] tlp 100 in-point ingress
```

Related Topics

21.4.25 nqa ipfpm dcp

21.4.17 instance (IPFPM-DCP view)

21.4.19 ipfpm tlp (layer 3 interface)

21.5 CWMP Configuration Commands

NOTE

The AR120 series (except AR129CV, AR129CVW and AR129CGVW-L) do not support CWMP.

21.5.1 cwmp

Function

The **cwmp** command displays the CWMP view.

Format

cwmp

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

On networks, too many devices are scattered on the user side and are hard to manage and maintain. To solve the preceding problems, CWMP defines a mechanism to manage the CPE by an ACS. This facilitates CPE management, reduces maintenance and operation costs, and improves troubleshooting efficiency.

The router functions as a CPE.

Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

Configure the CWMP function of the CPE.

Example

Enter the CWMP view.

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

Related Topics

21.5.15 cwmp enable

21.5.2 cwmp acs password

Function

The **cwmp acs password** command configures the password used to connect the CPE to the ACS.

The **undo cwmp acs password** command deletes the password.

By default, no password is available.

Format

cwmp acs password cipher

undo cwmp acs password

Parameters

Parameter	Description	Value
cipher	Displays the password in cipher text.	-

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent the transaction processing between CPEs and ACSs from being falsified and ensure the transaction processing confidentiality, the **cwmp acs password**

Copyright © Huawei Technologies Co., Ltd.

command is used to configure the authentication password used to connect the CPE to the ACS.

After the CPE sends an Inform message containing a URL to the ACS, the ACS authenticates the CPE using the user name and password. After being authenticated, the CPE can set up a connection with the ACS.

Precautions

The passwords must meet the following requirements:

- The password is a string of 6 to 255 case-sensitive characters.
- The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character.

  The special characters include spaces and the following:

  `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
- Password entered in interactive mode is not displayed on the screen.

After an active/standby switchover on the AR3200 routers, you need to run this command again to set a password.

Example

Set the password to abc123456.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp acs password cipher
Enter Password(<6-255>):
Confirm password:
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

21.5.25 display cwmp status

21.5.3 cwmp acs url

Function

The **cwmp acs url** command configures the URL used to connect the CPE to the ACS.

The **undo cwmp acs url** command deletes the URL.

By default, no URL is available.

Format

cwmp acs url *url*

undo cwmp acs url

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
url	Specifies the URL used to connect the CPE to the ACS.	The value is a string of 8 to 400 characters, in the format http://host[:port]/path or https://host[:port]/path. • host: IP address or domain name. • port: port number. The default value is **80**. Generally, the port number is added to the IP address or domain name only after the port number is changed. • path: working path of the HTTP server. The URL in the HTTPS format can ensure the communication security and data integrity between the ACS and CPE.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before setting up a connection with the ACS, the CPE needs to obtain the ACS URL. The **cwmp acs url** command configures the URL used to connect the CPE to the ACS.

After the CPE sends an Inform message containing the IP address of the CPE to the URL of the ACS, the ACS authenticates the CPE using the user name and password. After being authenticated, the CPE can set up a connection with the ACS.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the URL to http://www.acs.com/acs.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp acs url http://www.acs.com/acs
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

21.5.25 display cwmp status

21.5.4 cwmp acs username

Function

The **cwmp acs username** command configures the user name used to connect the CPE to the ACS.

The **undo cwmp acs username** command deletes the user name.

By default, no user name is available.

Format

cwmp acs username *username*

undo cwmp acs username

Parameters

Parameter	Description	Value
username	Specifies the user name used to connect the CPE to the ACS.	The value is a string of 1 to 255 case-sensitive characters. It cannot contain the following special characters: \ ? " #.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Copyright © Huawei Technologies Co., Ltd.

To prevent the transaction processing between CPEs and ACSs from being falsified and ensure the transaction processing confidentiality, the **cwmp acs username** command is used to configure the authentication user name used to connect the CPE to the ACS.

After the CPE sends an Inform message containing a URL to the ACS, the ACS authenticates the CPE using the user name and password. After being authenticated, the CPE can set up a connection with the ACS.

Example

Set the user name to newname.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp acs username newname
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

21.5.25 display cwmp status

21.5.5 cwmp cpe connect interface

Function

The **cwmp cpe connect interface** command configures the interface that a CPE uses to connect to an ACS.

The **undo cwmp cpe connect interface** command cancels the interface.

By default, the CPE automatically selects an interface from interfaces with reachable routes to the ACS to set up a CWMP connection with the ACS.

Format

cwmp cpe connect interface *interface-type interface-number*

undo cwmp cpe connect interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface connecting to an ACS.	-

Views

CWMP view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The Inform message sent by a CPE to an ACS contains the IP address of the specified interface. After authenticating the CPE, the ACS connects to this IP address and saves the IP address in its own address list. When the ACS initiates a connection with the CPE, the ACS sends an HTTP packet containing this IP address.

Generally, a CPE obtains a CWMP connection interface from all the interfaces to which the ACS have reachable routes. If the obtained interface does not connect the CPE to the ACS, CWMP connection fails to be set up. Therefore, a CWMP connection interface needs to be specified manually. You can use the **cwmp cpe connect interface** command to configure the interface.

After the CWMP connection interface is configured, the IP address of this interface is used as the source IP address of the CWMP connection.

Example

Specify GE 1/0/0 on the CPE to connect to the ACS.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe connect interface gigabitethernet 1/0/0
```

Related Topics

21.5.6 cwmp cpe connect retry

21.5.6 cwmp cpe connect retry

Function

The **cwmp cpe connect retry** command sets the number of attempts the CPE can make to retry a connection.

The **undo cwmp cpe connect retry** command restores the default number of attempts.

By default, the maximum number of attempts is 3.

Format

cwmp cpe connect retry *times*

undo cwmp cpe connect retry

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
times	Specifies the maximum number of attempts the CPE can make to retry a connection.	The value is an integer that ranges from 0 to 100. The value 0 indicates that the CPE does not retry a connection if the connection attempt fails.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the CPE fails to set up a connection with the ACS or a connection is interrupted unexpectedly, the CPE can be configured to automatically re-set up the connection. If the number of CPE auto-connection reattempts reaches the upper limit, the connection between the CPE and the ACS fails.

For the unstable link, you can increase the number of connection reattempts, which can be configured by the **cwmp cpe connect retry** command.

Example

Set the number of attempts the CPE can make to retry a connection to 5.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe connect retry 5
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

21.5.7 cwmp cpe inform interval

Function

The **cwmp cpe inform interval** command sets the interval at which the CPE sends Inform messages.

The **undo cwmp cpe inform interval** command restores the default interval.

Copyright © Huawei Technologies Co., Ltd.

By default, a CPE sends an Inform message every 600 seconds.

Format

cwmp cpe inform interval *seconds*

undo cwmp cpe inform interval

Parameters

Parameter	Description	Value
seconds	Specifies the interval at which a CPE sends Inform messages.	V200R010C00: The value is an integer that ranges from 30 to 86400, in seconds. V200R010C10 and later versions: The value is an integer that ranges from 30 to 172800, in seconds.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To set up a connection with an ACS, a CPE needs to send Inform messages. After an interval for sending the Inform messages is set by the **cwmp cpe inform interval** command, the CPE can automatically send Inform messages to the ACS at the interval.

Set a proper interval. If the interval is too short, the CPE frequently sends Inform messages to occupy network resources.

Prerequisites

The **cwmp cpe inform interval** command takes effect only after the **cwmp cpe inform interval enable** command is executed to enable periodic sending of Inform messages.

Example

Set the interval at which the CPE sends Inform messages to 800 seconds.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe inform interval 800
```

Related Topics

21.5.1 cwmp

21.5.8 cwmp cpe inform interval enable

21.5.22 display cwmp configuration

21.5.8 cwmp cpe inform interval enable

Function

The **cwmp cpe inform interval enable** command enables the CPE to periodically send Inform messages.

The **undo cwmp cpe inform interval enable** command disables the CPE from periodically sending Inform messages.

By default, the CPE does not periodically send Inform messages.

Format

cwmp cpe inform interval enable

undo cwmp cpe inform interval enable

Parameters

None

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To set up a connection with an ACS, a CPE needs to send Inform messages. After the function for the CPE to periodically send Inform messages is enabled by the **cwmp cpe inform interval enable** command, the CPE automatically sends Inform messages to the ACS.

After the CPE is enabled to periodically send Inform messages, set the interval using the **cwmp cpe inform interval** command. By default, a CPE sends an Inform message every 600 seconds.

Copyright © Huawei Technologies Co., Ltd.

Example

Enable the CPE to periodically send Inform messages.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe inform interval enable
```

Related Topics

21.5.1 cwmp

21.5.7 cwmp cpe inform interval

21.5.22 display cwmp configuration

21.5.9 cwmp cpe inform product-class device-type

Function

The **cwmp cpe inform product-class device-type** command adds the actual product type of the CPE to the session initiated by the CPE to the ACS.

The **undo cwmp cpe inform product-class device-type** command restores the default configuration.

By default, the session initiated by the CPE to the ACS contains the product type AccessRouter.

Format

cwmp cpe inform product-class device-type

undo cwmp cpe inform product-class device-type

Parameters

None

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

When the ACS needs to manage CPEs based on the product types of CPEs, use the **cwmp cpe inform product-class device-type** command to add the actual product types of CPEs to the sessions sent to the ACS. For example, the actual product types of CPEs include AR2220, AR2240C and AR2240.

Copyright © Huawei Technologies Co., Ltd.

Example

Add the actual product type of the CPE to the session initiated by the CPE to the ACS.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe inform product-class device-type
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

21.5.10 cwmp cpe inform time

Function

The **cwmp cpe inform time** command sets the time when a CPE sends an inform message.

The **undo cwmp cpe inform time** command cancels the time setting.

By default, no time is specified for the CPE to send an inform message.

Format

cwmp cpe inform time *time*

undo cwmp cpe inform time

Parameters

Parameter	Description	Value
time	Specifies the date and time when a CPE sends an inform message.	The value ranges from 1970-01-01T00:00:00 to 2105-12-31T23:59:59, in the format yyyy-mm-ddThh:mm:ss. The specified time must be later than the system time.

Views

CWMP view

Default Level

3: Management level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To set up a connection with an ACS, a CPE needs to send inform messages. After the time is set by the **cwmp cpe inform time** command, the CPE automatically sends an inform message to the ACS at the specified time.

Example

Configure the CPE to send an inform message at 2012-07-01 20:00:00.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe inform time 2012-07-01T20:00:00
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

21.5.11 cwmp cpe password

Function

The **cwmp cpe password** command configures the password used to connect an ACS to a CPE.

The **undo cwmp cpe password** command deletes the password.

By default, no password is available.

Format

cwmp cpe password cipher

undo cwmp cpe password

Parameters

Parameter	Description	Value
cipher	Displays the password in cipher text.	-

Views

CWMP view

Default Level

3: Management level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To prevent the transaction processing between CPEs and ACSs from being falsified and ensure the transaction processing confidentiality, the **cwmp cpe password** command is used to configure the authentication password used to connect the ACS to the CPE.

An ACS can send connection requests to a CPE at any time. After the ACS sends an HTTP packet containing the IP address of the CPE, the CPE authenticates the ACS using the user name and password. After being authenticated, the ACS can set up a connection with the CPE.

Precautions

The passwords must meet the following requirements:

- The password is a string of 6 to 255 case-sensitive characters.
- The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character.

  The special characters include spaces and the following:

  `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
- Password entered in interactive mode is not displayed on the screen.
- The password cannot be the same as the username.

After an active/standby switchover on the AR3200 routers, you need to run this command again to set a password.

Example

Set the password to abc123456.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe password cipher
Enter Password(<6-255>):
Confirm password:
```

Related Topics

21.5.12 cwmp cpe username

21.5.12 cwmp cpe username

Function

The **cwmp cpe username** command configures the user name used to connect the ACS to the CPE.

The **undo cwmp cpe username** command deletes the user name.

By default, no user name is available.

Format

cwmp cpe username *username*

Copyright © Huawei Technologies Co., Ltd.

undo cwmp cpe username

Parameters

Parameter	Description	Value
username	Specifies the user name used to connect the ACS to the CPE.	The value is a string of 1 to 255 case-sensitive characters, and cannot include invalid character \ ?.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

To prevent the transaction processing between CPEs and ACSs from being falsified and ensure the transaction processing confidentiality, the **cwmp cpe username** command is used to configure the authentication user name used to connect the ACS to the CPE.

An ACS can send connection requests to a CPE at any time. After the ACS sends an HTTP packet containing the IP address of the CPE, the CPE authenticates the ACS using the user name and password. After being authenticated, the ACS can set up a connection with the CPE.

Example

Set the user name to newname.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe username newname
```

Related Topics

21.5.11 cwmp cpe password

21.5.13 cwmp cpe wait timeout

Function

The **cwmp cpe wait timeout** command configures the connection timeout interval of the CPE. If no data is transmitted within the timeout interval, the connection between the CPE and ACS is torn down.

Copyright © Huawei Technologies Co., Ltd.

The **undo cwmp cpe wait timeout** command restores the default connection timeout interval.

By default, the connection timeout interval is 30 seconds.

Format

cwmp cpe wait timeout *seconds*

undo cwmp cpe wait timeout

Parameters

Parameter	Description	Value
seconds	Specifies the connection timeout interval.	The value is integer that ranges from 30 to 1800, in seconds.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The connection timeout interval is used in either of the following scenarios:

- After sending an Inform message to the ACS, if the CPE does not receive a response within the connection timeout interval, the CPE considers that the connection fails.
- After a connection is set up, if the CPE and the ACS do not exchange any messages within the connection timeout interval, the CPE considers that the connection is invalid and tears down the connection.

Example

Set the connection timeout interval of the CPE to 60 seconds.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe wait timeout 60
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

Copyright © Huawei Technologies Co., Ltd.

21.5.14 cwmp device-info serial-number system-mac

Function

The **cwmp device-info serial-number system-mac** command sets the serial number of a CPE to the system MAC address of the device.

The **undo cwmp device-info serial-number** command restores the default settings.

By default, the serial number of a CPE is the device ESN.

Format

cwmp device-info serial-number system-mac

undo cwmp device-info serial-number

Parameters

None

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The ACS can monitor various parameters of the CPE connected to the ACS. To ensure that the system MAC address is the serial number of the CPE, run the **cwmp device-info serial-number system-mac** command.

Precautions

If the CWMP session has been established, run the **cwmp device-info serial-number system-mac** or **undo cwmp device-info serial-number** command to re-establish a new CWMP session.

Example

Set the serial number of the CPE to the system MAC address of the device.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp device-info serial-number system-mac
```

 Copyright © Huawei Technologies Co., Ltd.

21.5.15 cwmp enable

Function

The **cwmp enable** command enables the CWMP function on a CPE.

The **undo cwmp enable** command disables the CWMP function on a CPE.

By default, the CWMP function is disabled on a CPE.

Format

cwmp enable

undo cwmp enable

Parameters

None

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

After the CWMP function is enabled for a CPE by the **cwmp enable** command, the CPE can be remotely managed by an ACS. The CWMP function facilitates CPE management, saves maintenance costs, and improves troubleshooting efficiency.

When a CPE is uploading or downloading files, the CWMP function on the CPE cannot be disabled.

Example

Disable the CWMP function on a CPE.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] undo cwmp enable
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

21.5.25 display cwmp status

Copyright © Huawei Technologies Co., Ltd.

21.5.16 cwmp escape-character

Function

The **cwmp escape-character** command adds a character to be translated.

The **undo cwmp escape-character** command deletes a character to be translated.

Format

cwmp escape-character *character characters*

undo cwmp escape-character *character*

Parameters

Parameter	Description	Value
character	Specifies a character to be translated.	The value is a case-sensitive character. It cannot be a space. **NOTE** The letter *e* or single quotation mark (") cannot be translated.
characters	Specifies a character (string) after translation.	The value is a string of 1 to 6 case-sensitive characters without any space. **NOTE** • The translated content cannot be double quotation marks (" ") or single quotation mark ("), but can be a character string containing double quotation marks, for example, "@". • However, translating a character into a character string containing double quotation marks may cause device exceptions; therefore, it is not recommended.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a configuration file contains special characters that are not supported by the ACS, the upload fails. To solve this problem, you can configure these characters to be translated into characters supported by the ACS on the CPE. The CPE then can upload the configuration file to the ACS successfully. You can run the **cwmp escape-character** command to add a character to be translated.

Copyright © Huawei Technologies Co., Ltd.

Precautions

- Currently, only 30 characters to be translated are supported. If more than 30 characters to be translated are configured, an error message is displayed.
- To make character translation take effect, run the **cwmp escape-character enable** command.

Example

Translate > into @.

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

Delete > to be translated.

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

Related Topics

21.5.1 cwmp

21.5.17 cwmp escape-character enable

21.5.17 cwmp escape-character enable

Function

The **cwmp escape-character enable** command enables the character translation function.

The **undo cwmp escape-character enable** command disables the character translation function.

By default, character translation is disabled.

Format

cwmp escape-character enable

undo cwmp escape-character enable

Parameters

None

Views

CWMP view

Default Level

3: Management level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

If you want to add or delete translated characters, first run the **cwmp escape-character enable** command to enable the character translation function.

Precautions

You can run the **cwmp escape-character** command to add or delete a translated character. New or deleted translation characters will not take effect until the **cwmp escape-character enable** command is used.

Example

Enable the character translation function.

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

Related Topics

21.5.1 cwmp

21.5.16 cwmp escape-character

21.5.18 cwmp password complexity-check disable

Function

The **cwmp password complexity-check disable** command disables complexity check on the passwords used for authentication between ACS and CPE.

The **undo cwmp password complexity-check disable** command enables complexity check on the passwords used for authentication between ACS and CPE.

By default, the complexity check on the passwords used for authentication between ACS and CPE is enabled.

Format

cwmp password complexity-check disable

undo cwmp password complexity-check disable

Parameters

None

Views

CWMP view

Default Level

3: Management level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When the complexity check function is enabled, the passwords entered in interactive mode for authentication between CPE and ACS must meet the following requirements:

- A password is a string of 6 to 255 case-sensitive characters.
- The password must be a combination of at least two of the following: uppercase letters, lowercase letters, digits, and special characters.

  Special characters include `~ ! @ # $ % ^ & * ( ) - _ = + \ | [{ }] ; : ' " , < . > /.

If you want to use simple passwords for CPE and ACS authentication, run the **cwmp password complexity-check disable** command to disable password complexity check. After the command is executed, the passwords configured using the **cwmp acs password cipher** and **cwmp cpe password cipher** commands do not need to meet complexity check requirements.

Precautions

To ensure security, do not disable complexity check on the passwords used for authentication between ACS and CPE.

Example

Disable complexity check on the passwords used for authentication between ACS and CPE.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp password complexity-check disable
```

21.5.19 cwmp permit interface

Function

The **cwmp permit interface** command specifies physical interfaces on the CPE to which the ACS can connect.

The **undo cwmp permit interface** command restores the default physical interfaces on the CPE to which the ACS can connect.

By default, the ACS can connect to all the physical interfaces on the CPE.

Format

cwmp permit interface { *interface-type interface-number* } &<1-5>

undo cwmp permit interface

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	*interface-type*: specifies the interface type. *interface-number*: specifies the interface number. *interface-number* and *interface-type* specify an interface.	-

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent the ACS from connecting to the CPE through an unauthorized physical interface, you can run the **cwmp permit interface** command to specify physical interfaces on the CPE to which the ACS can connect.

Precautions

- By default, the ACS can connect to all the physical interfaces on the CPE. When you run this command to specify one physical interface on the CPE, the ACS cannot connect to the other physical interfaces on the CPE.
- You can specify a maximum of five interfaces each time you run the **cwmp permit interface** command. The latest configuration overrides the previous one. For example, before you run the command, the ACS can connect to three physical interfaces GigabitEthernet 1/0/0, GigabitEthernet 2/0/0, and GigabitEthernet 3/0/0 on the CPE. After you run the command to specify the interface GigabitEthernet 1/0/0, the ACS can only connect to the interface GigabitEthernet 1/0/0.

Example

Specify physical interfaces on the CPE to which the ACS can connect.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp permit interface gigabitethernet 1/0/0 gigabitethernet 2/0/0
  Info: Succeeded in setting cwmp permit interface.
```

Restore the default physical interfaces on the CPE to which the ACS can connect.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] undo cwmp permit interface
```

 Copyright © Huawei Technologies Co., Ltd.

21.5.20 cwmp request upload current-configuration

Function

The **cwmp request upload current-configuration** command configures a CPE to upload the currently loaded configuration file to an ACS.

Format

cwmp request upload current-configuration

Parameters

None

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

After the connection between a CPE and an ACS is set up, the CPE needs to upload the currently loaded configuration file to the ACS. This function is configured by the **cwmp request upload current-configuration** command.

Example

Configure a CPE to upload the currently loaded configuration file to an ACS.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp request upload current-configuration
```

Related Topics

21.5.24 display cwmp request upload status

21.5.21 cwmp ssl-client

Function

The **cwmp ssl-client** command configures a certificate or policy for the HTTPS client.

The **undo cwmp ssl-client** command deletes the configured certificate or policy.

By default, no certificate or policy is configured for the HTTPS client.

Copyright © Huawei Technologies Co., Ltd.

Format

cwmp ssl-client { **client-root-cert** *rootcert-path1* [*rootcert-path2*] | **ssl-policy** *policy-name* }

undo cwmp ssl-client { **client-root-cert** | **ssl-policy** }

Parameters

Parameter	Description	Value
client-root-cert *rootcert-path1 rootcert-path2*	Configures the CPE to validate the certificate from the ACS. ● *rootcert-path1*: Specifies the absolute path of the level-1 root certificate. The level-1 root certificate is issued by the certification association (CA). ● *rootcert-path2*: Specifies the absolute path of the level-2 root certificate. The Level-2 root certificate is used for communication between devices.	The value is a string of 1 to 64 case-sensitive characters. It cannot contain any space or question mark (?).
ssl-policy *policy-name*	Configures the CPE to validate the SSL policy from the ACS.	The value is a string of 1 to 31 case-insensitive characters. It cannot contain any space or question mark (?).

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Security Socket Layer (SSL) ensures communication security and data integrity between the ACS and CPE.

Copyright © Huawei Technologies Co., Ltd.

When the ACS URL is in the HTTPS format, the CPE and ACS must authenticate each other, and the SSL connection is set up only after the CPE and ACS are authenticated. It ensures the confidentiality of communication between the ACS and the CPE and data integrity.

NOTE

Before configuring a CPE to authenticate the ACS using an SSL policy, run the **ssl policy** *policy-name* command to configure the SSL policy on the CPE.

Precautions

The system time must be correctly set; otherwise, certificate validation may fail. To use a new certificate, uninstall the existing certificate first.

Example

Load the root certificate Interop_CA.cer.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp ssl-client client-root-cert flash:/Interop_CA.cer
Info: Succeed to load the trusted CA certificate.
[Huawei-cwmp]
```

21.5.22 display cwmp configuration

Function

The **display cwmp configuration** command displays the CWMP configurations on a CPE.

Format

display cwmp configuration

Parameters

None

Views

All view

Default Level

3: Management level

Usage Guidelines

None

Example

Display the CWMP configurations on a CPE.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display cwmp configuration
  CWMP is enabled
  ACS URL:                    http://www.acs.com:80/acs
  ACS username:                  hwcpe
  ACS password:                  %@%@x:J6T3+\>-7JE_7mDOKM,v`c%@%@
  Inform enable status:          disabled
  Inform interval:               600s
  Inform time:                   -
  Wait timeout:                  30s
  Reconnection times:            3
```

Table 21-31 Description of the **display cwmp configuration** command output

Item	Description
CWMP is enabled	CWMP (TR-069) is enabled. • enable: CWMP is enabled. • disabled: CWMP is disabled. This item can be configured by the **cwmp enable** command.
ACS URL	ACS's URL to which the CPE connects. If no URL is configured, the system displays -. This item can be configured by the **cwmp acs url** command.
ACS username	Authentication user name of the ACS. If no user name is configured, the system displays -. This item can be configured by the **cwmp acs username** command.
ACS password	Authentication password of the ACS. If no password is configured, the system displays -. This item can be configured by the **cwmp acs password** command.
Inform enable status	Whether the CPE is configured to periodically send Inform messages. This item can be configured by the **cwmp cpe inform interval enable** command.
Inform interval	Interval at which the CPE sends Inform messages. This item can be configured by the **cwmp cpe inform interval** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Inform time	Time when the CPE sends an Inform message. If no time is specified, the system displays -. This item can be configured by the **cwmp cpe inform time** command.
Wait timeout	Close-wait timer of the CPE. This item can be configured by the **cwmp cpe wait timeout** command.
Reconnection times	Maximum number of attempts the CPE can make to retry a connection. This item can be configured by the **cwmp cpe connect retry** command.

Related Topics

21.5.2 cwmp acs password
21.5.3 cwmp acs url
21.5.4 cwmp acs username
21.5.7 cwmp cpe inform interval
21.5.8 cwmp cpe inform interval enable
21.5.10 cwmp cpe inform time
21.5.13 cwmp cpe wait timeout
21.5.6 cwmp cpe connect retry
21.5.15 cwmp enable

21.5.23 display cwmp password

Function

The **display cwmp password** command displays the password that the CPE uses to connect to the ACS, and the password that the ACS uses to connect to the CPE.

Format

display cwmp password

Parameters

None

Views

CWMP view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

This command is used to view the password that the CPE uses to connect to the ACS and the password that the ACS uses to connect to the CPE.

Example

Display the passwords that the CPE and the ACS use to connect to each other.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] display cwmp password
 cwmp cpe password %@%@=;fNL1~b)Z:v/&#DBe^0$y7!%@%@
 cwmp acs password %@%@H6^EXz:*EP-!'->Apla@$xZK%@%@
```

Table 21-32 Description of the display cwmp password command output

Item	Description
cwmp cpe password	Password that the ACS uses to connect to the CPE.
cwmp acs password	Password that the CPE uses to connect to the ACS.

Related Topics

21.5.2 cwmp acs password

21.5.11 cwmp cpe password

21.5.24 display cwmp request upload status

Function

The **display cwmp request upload status** command displays the status of the configuration file uploaded from a CPE to an ACS.

Format

display cwmp request upload status

Parameters

None

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

This command is used to view the status of the configuration file uploaded from a CPE to an ACS. The command output and description are as follows:

- **Success to upload the current configuration file**: indicates that the configuration file has been uploaded to the ACS.
- **The current configuration file is uploading**: indicates that the configuration file is being uploaded to the ACS.
- **Failed to upload the current configuration file**: indicates that the configuration file fails to be uploaded to the ACS.

Example

Display the status of the configuration file uploaded from a CPE to an ACS.

```
<Huawei> display cwmp request upload status
Success to upload the current configuration file.
```

Related Topics

21.5.20 cwmp request upload current-configuration

21.5.25 display cwmp status

Function

The **display cwmp status** command displays the CWMP status on a CPE.

Format

display cwmp status

Parameters

None

Views

All view

Default Level

3: Management level

Usage Guidelines

None

Copyright © Huawei Technologies Co., Ltd.

Example

Display the CWMP status on a CPE.

```
<Huawei> display cwmp status
 CWMP is enabled
 ACS URL:                          -
 ACS information is set by:          user
 ACS username:                     -
 ACS password:                     -
 Connection status:                disconnected
 Time of last successful connection:   -
```

Table 21-33 Description of the **display cwmp status** command output

Item	Description
CWMP is enabled	CWMP (TR-069) is enabled. • enable: CWMP is enabled. • disabled: CWMP is disabled. This item can be configured by the **cwmp enable** command.
ACS URL	ACS's URL to which the CPE connects. If no URL is configured, the system displays -. This item can be configured by the **cwmp acs url** command.
ACS information is set by	How the CPE obtains the ACS's URL. • user: The ACS's URL is configured using a command. • acs: The URL is sent by the ACS to the CPE. • dhcp: The URL is sent by the ACS to a DHCP server.
ACS username	Authentication user name of the ACS. If no user name is configured, the system displays -. This item can be configured by the **cwmp acs username** command.
ACS password	Authentication password of the ACS. If no password is configured, the system displays -. This item can be configured by the **cwmp acs password** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Connection status	Status of a connection between the CPE and the ACS: • connected: The connection has been set up successfully. • disconnected: The connection has not been set up. • waiting response: The CPE is waiting for the response packet from the ACS.
Time of last successful connection	Time when the last connection is set up. If no connection has been set up, the system displays -.

Related Topics

21.5.2 cwmp acs password
21.5.3 cwmp acs url
21.5.4 cwmp acs username
21.5.15 cwmp enable

21.5.26 cwmp ip-change inform disable

Function

The **cwmp ip-change inform disable** command disables the device from informing the ACS of an IP address change event.

The **undo cwmp ip-change inform disable** command enables the device to inform the ACS of an IP address change event.

By default, when the IP address of a device changes, the device does not inform the ACS of this event.

Format

cwmp ip-change inform disable

undo cwmp ip-change inform disable

Parameters

None

Views

CWMP view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **cwmp ip-change inform disable** command to disable the device from informing the ACS of an IP address change event.

Precautions

This command takes effect only on IP addresses reachable to the ACS.

Example

Disable the device from informing the ACS of an IP address change event.

```
<Huawei> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei] cwmp
[Huawei-cwmp] cwmp ip-change inform disable
```

Related Topics

21.5.1 cwmp

21.5.27 cwmp ssl-server ssl-policy

Function

The **cwmp ssl-server ssl-policy** command binds an SSL server policy to CWMP.

The **undo cwmp ssl-ser ssl-policy** command unbinds an SSL server policy from CWMP.

By default, no SSL server policy is bound to CWMP.

Format

cwmp ssl-server ssl-policy *policy-name*

undo cwmp ssl-server ssl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL server policy.	The value is a string of 1 to 31 case-insensitive characters. It cannot contain spaces or question marks (?).

Copyright © Huawei Technologies Co., Ltd.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an ACS initiates a connection with a CPE, you can configure a transport-layer security protocol to ensure communication data security and integrity. Hypertext Transfer Protocol Secure (HTTPS) supports the Secure Sockets Layer (SSL) protocol. Run the **cwmp ssl-server ssl-policy** *policy-name* command to bind an SSL policy to CWMP, so that the ACS can set up HTTPS connections. After this command is executed, run the **display ssl ssl-policy** command to view the binding information of SSL server policy.

Precautions

1. The connection is initiated by the server, so the SSL policy type must be server; otherwise, the SSL connection cannot be set up. Run the **ssl policy** *policy-name* [**type** { **client** | **server** }] command to configure the SSL server policy.
2. Before binding an SSL server policy to CWMP, run the **pki-realm** *realm-name* command to specify the PKI realm for the SSL policy.

Example

Bind the SSL server policy to CWMP.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp ssl-server ssl-policy Test3Server
Info:Succeed to bind ssl policy.
```

21.6 LLDP Configuration Commands

21.6.1 display lldp local

Function

The **display lldp local** command displays global LLDP information or the LLDP information on a specified interface.

Format

display lldp local [**interface** *interface-type interface-number*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the LLDP information on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, the command displays LLDP information on all the interfaces with LLDP enabled.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display lldp local** command displays the global LLDP information or the LLDP information on an interface.

- The global LLDP information includes system information, MED system information, system configuration, and data statistics on the peer device.
- The LLDP information on the Ethernet interface, and port group include the interface information and MED interface information, The LLDP information on the Serial interface includes the interface information.

To verify the LLDP information and Layer 2 information of the system and interfaces, run this command.

Prerequisites

The LLDP function has been enabled globally and on the specified interface.

Example

Display the global LLDP information.

```
<Huawei> display lldp local
System information
Chassis type   :macAddress
Chassis ID     :00e0-11fc-1710
System name    :Huawei
System description  :Huawei AR2240 Huawei Versatile Routing Platform Software  V
RP (R) software,Version 5.120 (AR2240 V200R010 ) Copyright (C) 2011-2013 Huawei
 Technologies Co., Ltd
System capabilities supported   :bridge
System capabilities enabled     :bridge
LLDP Up time   :2012/05/10 11:40:49
```

 Copyright © Huawei Technologies Co., Ltd.

```
MED system information
Device class   :Network Connectivity
(MED inventory information of master board)
HardwareRev       :AR01SRU1A VER.A
FirmwareRev       :404
SoftwareRev       :V200R010
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

System configuration
LLDP Status                  :enabled            (default is disabled)
LLDP Message Tx Interval     :30                 (default is 30s)
LLDP Message Tx Hold Multiplier :4               (default is 4)
LLDP Refresh Delay           :2                  (default is 2s)
LLDP Tx Delay                :2                  (default is 2s)
LLDP Notification Interval   :5                  (default is 5s)
LLDP Notification Enable     :enabled            (default is enabled)
Management Address           :IP: 10.10.10.1  MAC: 00e0-11fc-1710

Remote Table Statistics:
Remote Table Last Change Time   :0 days, 5 hours, 57 minutes, 32 seconds

Remote Neighbors Added          :15

Remote Neighbors Deleted        :13

Remote Neighbors Dropped        :0

Remote Neighbors Aged           :0

Total Neighbors                 :2


Port information:
Interface GigabitEthernet1/0/0:
LLDP Enable Status       :enabled            (default is disabled)
Total Neighbors          :0

Port ID subtype     :interfaceName
Port ID             :GigabitEthernet1/0/0
Port description    :HUAWEI, AR Series, GigabitEthernet1/0/0 Interface

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :9216

MED port information

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0

Interface Ethernet2/0/0:
LLDP Enable Status       :enabled            (default is disabled)
```

 Copyright © Huawei Technologies Co., Ltd.

```
Total Neighbors          :1

Port ID subtype     :interfaceName
Port ID             :Ethernet2/0/0
Port description    :HUAWEI, AR Series, Ethernet2/0/0 Interface

Port And Protocol VLAN ID(PPVID) don't supported
Port VLAN ID(PVID)  :1
VLAN name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP GVRP

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :9216

MED port information

Media policy type   :Voice
Unknown Policy      :Defined
VLAN tagged         :Yes
Media policy VlanID          :0
Media policy L2 priority     :6
Media policy Dscp            :46

Power Type              :Unknown
PoE PSE power source    :Unknown
Port PSE Priority       :Unknown
Port Available power value:2
  ---- More ----
```

Table 21-34 Description of the display lldp local command output.

Item	Description
System information	
Chassis type	Device ID sub-type: • chassisComponent: chassis alias • interfaceAlias: interface alias • portComponent: interface or backplane alias • macAddress: MAC address • networkAddress: network address • InterfaceName: name of the interface • local: name of the local device
Chassis ID	Device ID.
System name	Name of the device.
System description	Device description.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
System capabilities supported	Capabilities of the local device, including: • repeater: repeater • bridge: bridge device • wlanAccessPoint: wireless access point • router: router • telephone: wireless device • docsisCableDevice: management station • stationOnly: base station • other: other capabilities
System capabilities enabled	Capabilities enabled on the local device, including: • repeater: repeater • bridge: bridge device • wlanAccessPoint: wireless access point • router: router • telephone: wireless device • docsisCableDevice: management station • stationOnly: base station • other: other capabilities
LLDP Up time	Time when LLDP is enabled.
MED system information	
Device class	Type of the MED device.
HardwareRev	Hardware version of the device.
FirmwareRev	Firmware version of the product.
SoftwareRev	Software version of the device.
SerialNum	Serial number.
Manufacturer name	Name of the manufacturer
Model name	Name of a model.
Asset tracking identifier	Asset tracking ID.
System configuration	
LLDP Status	LLDP status: • Enabled • Disabled This parameter is configured using the **lldp enable (system view)** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
LLDP Message Tx Interval	Interval for sending LLDP packets. This parameter is configured using the **lldp message-transmission interval** command.
LLDP Message Tx Hold Multiplier	Multiplier of the period in which the message is held. This parameter is configured using the **lldp message-transmission hold-multiplier** command.
LLDP Refresh Delay	Delay in re-initializing the LLDP module. This parameter is configured using the **lldp restart-delay** command.
LLDP Tx Delay	Delay in sending the LLDP packets. This parameter is configured using the **lldp message-transmission delay** command.
LLDP Notification Interval	Delay in sending the notification after the remote information changes. This parameter is configured using the **lldp trap-interval** command.
LLDP Notification Enable	Status of the notification function. • Enabled • Disabled
Management Address	Management address. This parameter is configured using the **lldp management-address** command.
Remote Table Statistics	
Remote Table Last Change Time	Time that elapsed since the latest modification of remote data.
Remote Neighbors Added	Number of added remote neighbors.
Remote Neighbors Deleted	Number of deleted remote neighbors.
Remote Neighbors Dropped	Number of remote neighbors discarded after the buffer is used up.
Remote Neighbors Aged	Number of neighbors that are aged out and deleted.
Total Neighbors	Number of remote neighbors.
Port information	

Copyright © Huawei Technologies Co., Ltd.

Item	Description
LLDP Enable Status	LLDP status: ● Enabled ● Disabled
Total Neighbors	Number of remote neighbors.
Port ID subtype	Subtypes of a port ID. ● interfaceAlias: interface alias ● portComponent: interface or backplane alias ● macAddress: MAC address ● networkAddress: network address ● InterfaceName: name of the interface ● agentCircuitId: circuit ID of the DHCP agent ● local: name of the local device
Port ID	Interface ID.
Port description	Interface description.
Port VLAN ID(PVID)	VLAN ID of the interface.
VLAN name of VLAN 1	Name of VLAN 1.
Protocol identity	Protocol ID.
Auto-negotiation supported	Whether the interface supports auto-negotiation: ● Yes ● No
Auto-negotiation enabled	Whether the interface is enabled with auto-negotiation: ● Yes ● No
OperMau	Auto-sensing rate and duplex mode of the interface.
Power port class	PoE type: ● PSE: power-sourcing equipment ● PD: powered device
PSE power supported	Whether the PSE power is supported. ● Yes: PSE power is supported. ● No: PSE power is not supported.
PSE power enabled	Whether the PSE power is enabled. ● Yes: enabled. ● No: disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PSE pairs control ability	Whether the PSE twisted pair control is supported. ● Yes: PSE twisted pair control is supported. ● No: PSE twisted pair control is not supported.
Power pairs	PoE remote power supply mode. ● Signal: power supply mode of signal lines ● Spare: power supply mode of spare signal lines ● Unknown: an unknown remote power supply mode
Port power classification	PD power control level on the interface: ● Class0: indicates level 1. ● Class1: indicates level 2. ● Class2: indicates level 3. ● Class3: indicates level 4. ● Class4: indicates level 5. ● Unknown: indicates an unknown level.
Link aggregation supported	Whether the interface supports link aggregation. ● Yes: The interface supports link aggregation. ● No: The interface does not support link aggregation.
Link aggregation enabled	Whether link aggregation is enabled on the interface. ● Yes: enabled ● No: disabled
Aggregation port ID	ID of an aggregated interface, If link aggregation is disabled, the value of this field is 0.
Maximum frame Size	Maximum size of a frame supported by the interface.
MED port information	
Media policy type	Type of the media policy: ● voice: indicates that the device supports voice. ● unknown: indicates that the type of the media policy is unknown.
Unknown Policy	Whether the type of the media policy is unknown: ● Yes: unknown ● Defined: known

Copyright © Huawei Technologies Co., Ltd.

Item	Description
VLAN tagged	Whether to add tag to the packets of the voice VLAN. • Yes: Adds a VLAN tag to packets of the voice VLAN. • No: Not to add a VLAN tag to packets of the voice VLAN.
Media policy VlanID	ID of the voice VLAN.
Media policy L2 priority	Layer 2 priority.
Media policy Dscp	DSCP value.
Power Type	Power supply type.
PoE PSE power source	Type of the PSE: • Primary: indicates primary power supply. • Backup: indicates backup power supply. • Unknown: indicates power supply of an unknown type.
Port PSE Priority	PSE priority of an interface: • Unknown: indicates an unknown priority. • Critical: indicates the highest priority. • High: indicates the medium priority. • Low: indicates the lowest priority.
Port Available power value	Port power supply.

Related Topics

21.6.10 lldp enable (system view)

21.6.2 display lldp neighbor

Function

The **display lldp neighbor** command displays information about neighboring device of all interfaces or a specified interface.

Format

display lldp neighbor [**interface** *interface-type interface-number*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about neighboring devices of a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If no interface is specified, the command displays information about neighboring devices of all interfaces with LLDP enabled.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Using this command, you can know which neighboring devices are connected to the local device, to which interfaces the neighboring devices are connected, layer 2 information about the neighbors, and whether LLDP configuration is correct.

Prerequisites

The LLDP function has been enabled globally and on the specified interface.

Example

Display information about neighbor devices of interfaces Ethernet2/0/0.

```
<Huawei> display lldp neighbor interface ethernet 2/0/0
Ethernet2/0/0 has 1 neighbors:

Neighbor index : 1
Chassis type    :macAddress
Chassis ID      :00e0-11fc-1710
Port ID type    :interfaceName
Port ID         :Ethernet2/0/0
Port description    :HUAWEI, AR Series, Ethernet2/0/0 Interface
```

 Copyright © Huawei Technologies Co., Ltd.

```
System name         :Huawei
System description  :Huawei AR2240 Huawei Versatile Routing Platform Software  V
RP (R) software,Version 5.120 (AR2240 V200R010) Copyright (C) 2011-2013 Huawei
 Technologies Co., Ltd
System capabilities supported   :bridge
System capabilities enabled     :bridge
Management address type  :ipV4
Management address       : 10.0.0.1
Expired time   :104s


Port VLAN ID(PVID)  :1
VLAN name of VLAN  1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP GVRP

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :9216

MED Device information
Device class   :Network Connectivity

HardwareRev       :AR01SRU1A VER.A
FirmwareRev       :100
SoftwareRev       :V200R010
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

Media policy type   :Voice
Unknown Policy      :Defined
VLAN tagged         :Yes
Media policy VlanID      :0
Media policy L2 priority :6
Media policy Dscp        :46

Power Type              :Unknown
PoE PSE power source    :Unknown
Port PSE Priority       :Unknown
Port Available power value:2
```

Table 21-35 Description of the display lldp neighbor command output

Item	Description
Neighbor index	Index of a neighbor.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Chassis type	ID sub-types of a neighboring device: • chassisComponent: chassis alias • interfaceAlias: interface alias • portComponent: interface or backplane alias • macAddress: MAC address • networkAddress: network address • InterfaceName: name of the interface • local: name of the local device
Chassis Id	ID of a neighboring device.
Port ID type	ID sub-type of a neighboring interface: • interfaceAlias: interface alias • portComponent: interface or backplane alias • macAddress: MAC address • networkAddress: network address • InterfaceName: name of the interface • agentCircuitId: circuit ID of the DHCP agent • local: name of the local device
Port Id	ID of a neighbor interface.
Port description	Description of a neighboring interface.
System name	System name of a neighboring device.
System description	Description of a neighboring device.
System capabilities supported	Capabilities of a neighboring device (at least one capability is supported): • other: other capabilities • repeater: repeater • bridge: bridge device • wlanAccessPoint: wireless access point • router: router • telephone: wireless device • docsisCableDevice: management station • stationOnly: base station

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
System capabilities enabled	Capabilities enabled on a neighboring device (This field is a subset of the system capabilities supported field, and at least one capability must be enabled). ● other: other capabilities ● repeater: repeater ● bridge: bridge device ● wlanAccessPoint: wireless access point (AP) ● router: router ● telephone: wireless device ● docsisCableDevice: management station ● stationOnly: base station
Management address type	Type of the management address.
Management address	Management address of a neighbor.
Expired time	Aging time of a neighbor.
Port VLAN ID(PVID)	VLAN ID of an interface.
Protocol identity	Protocol ID.
VLAN name of VLAN 1	Name of VLAN 1.
Auto-negotiation supported	Whether the interface supports auto-negotiation: ● Yes: Auto-negotiation is supported. ● No: Auto-negotiation is not supported.
Auto-negotiation enabled	Whether the interface is enabled with auto-negotiation: ● Yes: enabled. ● No: disabled.
OperMau	Transmission rate and duplex mode of the interface.
Power port class	PoE type: ● PSE: power-sourcing equipment. ● PD: powered device.
PSE power supported	Whether the PSE power is supported. ● Yes: PSE power is supported. ● No: PSE power is not supported.
PSE power enabled	Whether the PSE power is enabled. ● Yes: enabled. ● No: disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PSE pairs control ability	Whether the PSE control is supported. ● Yes: PSE control is supported. ● No: PSE control is not supported.
Power pairs	PoE remote power supply mode. ● Signal: power supply mode of signal lines. ● Spare: power supply mode of spare signal lines. ● Unknown: an unknown remote power supply mode.
Port power classification	PD power control level on the interface: ● Class0: indicates level 1. ● Class1: indicates level 2. ● Class2: indicates level 3. ● Class3: indicates level 4. ● Class4: indicates level 5. ● Unknown: indicates an unknown control level.
Link aggregation supported	Whether link aggregation is supported on the interface. ● Yes: The interface supports link aggregation. ● No: The interface does not support link aggregation.
Link aggregation enabled	Whether link aggregation is enabled on an interface. ● Yes: The interface supports link aggregation. ● No: The interface does not support link aggregation.
Aggregation port ID	ID of an aggregated interface, If link aggregation is disabled, the value of this field is 0.
Maximum frame Size	Maximum size of a frame supported by the interface.
Device class	Type of the MED device.
HardwareRev	Hardware version of the product.
FirmwareRev	Firmware version of the product.
SoftwareRev	Software version of the product.
SerialNum	Serial number.
Manufacturer name	Name of the manufacturer.
Model name	Name of a model.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Asset tracking identifier	Asset tracking ID.
Media policy type	Type of the media policy: • voice: indicates that the device supports voice. • unknown: indicates that the type of the media policy is unknown.
Unknown Policy	Whether the type of the media policy is unknown. Yes indicates that the media policy type is unknown. No indicates that the media policy type is known.
VLAN tagged	Whether to add tag to the packets of the voice VLAN.
Media policy VlanID	ID of the voice VLAN.
Media policy L2 priority	Layer 2 priority.
Media policy Dscp	DSCP value.
Power Type	Power supply type: • PSE: power-sourcing equipment. • PD: powered device.
PoE PSE power source	Type of the PSE: • Primary: indicates primary power supply. • Backup: indicates backup power supply. • Unknown: indicates power supply of an unknown type.
Port PSE Priority	PSE priority of an interface: • Unknown: indicates an unknown priority. • Critical: indicates the highest priority. • High: indicates the medium priority. • Low: indicates the lowest priority.
Port Available power value	Port power supply

Related Topics

21.6.10 lldp enable (system view)

 Copyright © Huawei Technologies Co., Ltd.

21.6.3 display lldp neighbor brief

Function

The **display lldp neighbor brief** command displays brief information about neighbors of the device.

Format

display lldp neighbor brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To quickly view the neighbors of the local device and the interfaces connected to neighbors, run this command.

Prerequisites

The LLDP function has been enabled globally.

Example

Display information about neighbor devices.

```
<Huawei> display lldp neighbor brief
Local Intf   Neighbor Dev          Neighbor Intf          Exptime
Eth2/0/0     Huawei                Eth0/0/2               103
```

Table 21-36 Description of the display lldp neighbor brief command output

Item	Description
Local Intf	Local interface.
Neighbor Dev	Name of neighbor device.
Neighbor Intf	Neighboring interface.
Exptime	Aging time of a neighbor, in seconds.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.6.2 display lldp neighbor

21.6.10 lldp enable (system view)

21.6.4 display lldp statistics

Function

The **display lldp statistics** command displays statistics about LLDP packets sent and received by all or a specified interface.

Format

display lldp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about LLDP packet sent and received by a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If no interface is specified, the command displays statistics about LLDP packets on all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display lldp statistics** command displays the statistics about sent and received LLDP packets.

Copyright © Huawei Technologies Co., Ltd.

To display the LLDP packet statistics within a specified period of time, run the **reset lldp statistics** command to clear the existing statistics first, and then run the **display lldp statistics** command to display the new statistics.

Prerequisites

The LLDP function has been enabled globally and on interfaces.

Precautions

If the LLDP function is enabled globally but disabled on an interface, the packet statistics on the interface are 0.

Example

Display the statistics about sent and received LLDP packets on all interfaces.

```
<Huawei> display lldp statistics
LLDP statistics global Information:
Statistics for Ethernet2/0/0:
Transmitted Frames Total: 2839
Received Frames Total:    2728      Frames Discarded Total:  0
Frames Error Total:       0         TLVs Discarded Total:    0
TLVs Unrecognized Total:  0         Neighbors Expired Total: 0
```

Table 21-37 Description of the display lldp statistics command output

Item	Description
Transmitted Frames Total	Number of sent LLDP packets.
Received Frames Total	Number of received LLDP packets.
Frames Discarded Total	Number of discarded LLDP packets.
Frames Error Total	Number of received errored LLDP packets.
TLVs Discarded Total	Number of discarded TLVs.
TLVs Unrecognized Total	Number of unknown TLVs.
Neighbors Expired Total	Number of aged-out neighbors.

Related Topics

21.6.10 lldp enable (system view)
21.6.19 reset lldp statistics

21.6.5 display lldp tlv-config

Function

The **display lldp tlv-config** command displays optional TLVs that can be sent with LLDP packets on all or a specified interface.

Format

display lldp tlv-config [**interface** *interface-type interface-number*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays optional TLVs supported by a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If no interface is specified, the command displays optional TLVs on all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display lldp tlv-config** command displays the TLVs supported by the specified interface or all interfaces, and thus you can know whether the required TLVs are enabled and unneeded TLVs are disabled.

Prerequisites

The LLDP function has been enabled globally and on interfaces.

Example

Display Optional TLVs that can be sent with LLDP packets on Ethernet2/0/0.

```
<Huawei> display lldp tlv-config interface ethernet 2/0/0
LLDP tlv-config of port [Ethernet2/0/0]:
Name                          Status    Default
Basic optional TLV:
Port Description TLV             Yes       Yes
System Name TLV                  Yes       Yes
System Description TLV           Yes       Yes
System Capabilities TLV          Yes       Yes
Management Address TLV           Yes       Yes
IEEE 802.1 extend TLV:
Port VLAN ID TLV                 Yes       Yes
Port And Protocol VLAN ID TLV    Yes       Yes
VLAN Name TLV                    Yes       Yes
```

 Copyright © Huawei Technologies Co., Ltd.

```
Protocol identity TLV             Yes       Yes
IEEE 802.3 extend TLV:
MAC-Physic TLV                    Yes       Yes
Power via MDI TLV                 Yes       Yes
Link Aggregation TLV              Yes       Yes
Maximum Frame Size TLV            Yes       Yes
LLDP-MED extend TLV:
Capabilities TLV                  Yes       Yes
Network Policy TLV                Yes       Yes
Extended Power via MDI TLV        Yes       Yes
Inventory TLV                     Yes       Yes
Location Identification TLV       No        No
```

Table 21-38 Description of the display lldp tlv-config command output

Item	Description
Name	Type of TLV.
Status	Whether the interface is configured to send the TLVs of the specified type.
Default	Whether the TLVs of the specified types are sent on an interface by default.
Basic optional TLV	Basic TLVs that can be sent on an interface.
Port Description TLV	Interface description TLV.
System Name TLV	System name TLV.
System Description TLV	System description TLV.
System Capabilities TLV	TLV indicating the system capability set.
Management Address TLV	Management address TLV.
IEEE 802.1 extend TLV	Type of the IEEE 802.1 organizational-specific TLVs that can be sent on an interface.
Port VLAN ID TLV	PVID TLV.
Port And Protocol VLAN ID TLV	Port and protocol VLAN ID TLV.
VLAN Name TLV	VLAN name TLV.
Protocol identity TLV	Protocol ID TLV.
IEEE 802.3 extend TLV	IEEE 802.3 organizational-specific TLVs that can be sent on an interface.
MAC-Physic TLV	TLV indicating physical attributes of an interface.
Power via MDI TLV	Power capability TLV.
Link Aggregation TLV	Link aggregation TLV.
Maximum Frame Size TLV	Maximum frame length TLV.
LLDP-MED extend TLV	LLDP MED TLV.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Capabilities TLV	TLV indicating MED capability sets.
Extended Power via MDI TLV	TLV indicating the extended power supply capabilities.
Inventory TLV	Inventory information, including Hardware Revision TLV, Firmware Revision TLV, Software Revision TLV, Serial Number TLV, Manufacturer Name TLV, Model name TLV, and Asset id TLV.
Network Policy TLV	Network policy TLV.
Location Identification TLV	Location ID TLV.

21.6.6 display snmp-agent trap feature-name lldptrap all

Function

The **display snmp-agent trap feature-name lldptrap all** command displays the status of all traps on the LLDP module.

Format

display snmp-agent trap feature-name lldptrap all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running the **display snmp-agent trap feature-name lldptrap all** command, run the **snmp-agent** command to enable the SNMP Agent function.

Example

Display the status of all traps on the LLDP module.

```
<Huawei> display snmp-agent trap feature-name lldptrap all
------------------------------------------------------------------------------
Feature name: LLDPTRAP
Trap number : 4
```

 Copyright © Huawei Technologies Co., Ltd.

```
------------------------------------------------------------------------------
Trap name                 Default switch status   Current switch status
lldpRemTablesChange           on                      on
hwLldpEnabled                 on                      on
hwLldpDisabled                on                      on
hwLldpLocManIPAddrChange      on                      on
```

Table 21-39 Description of the **display snmp-agent trap feature-name lldptrap all** command output

Item	Description
Feature name	Name of the module to which a trap belongs.
Trap number	Number of traps.
Trap name	Names of a trap, traps of the LLDP module include: • lldpRemTablesChange: Sends a trap when LLDP neighbor information changes. • hwLldpEnabled: Sends a Huawei proprietary trap when the LLDP function is enabled globally. • hwLldpDisabled: Sends a Huawei proprietary trap when the LLDP function is disabled globally. • hwLldpLocManIPAddrChange: Sends a Huawei proprietary trap when the LLDP management address of the device changes.
Default switch status	Default status of a trap: • on: The trap is enabled. • off: The trap is disabled.
Current switch status	Status of a trap: • on: The trap is enabled. • off: The trap is disabled.

Related Topics

21.6.20 snmp-agent trap enable feature-name lldptrap

21.6.7 lldp clear neighbor

Function

The **lldp clear neighbor** command clears neighbor information in the system or on an interface.

Format

lldp clear neighbor [**interface** *interface-type interface-number*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Indicates the type and number of the interface whose neighbor information to be cleared. In the command: • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If no interface is specified, neighbor information of all interfaces is cleared.	-

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If you want to obtain the latest neighbor information of interfaces, use the **lldp clear neighbor** command to clear existing neighbor information. When an interface receives new packets, new neighbor information is generated.

Prerequisites

The LLDP function has been enabled globally and on interfaces.

Example

Clear neighbor information of all interfaces.

```
<Huawei> lldp clear neighbor
Warning: This command will clear the neighbor information of all the ports. Continue? [Y/N]y
```

Related Topics

21.6.1 display lldp local

21.6.2 display lldp neighbor

21.6.3 display lldp neighbor brief

Copyright © Huawei Technologies Co., Ltd.

21.6.9 lldp enable (interface view)
21.6.10 lldp enable (system view)

21.6.8 lldp dot3-tlv power

Function

The **lldp dot3-tlv power** command sets the standard to which the 802.3 Power via MDI TLV sent by an interface conforms.

By default, the 802.3 Power via MDI TLV conforms to 802.1 ab.

Format

lldp dot3-tlv power { **802.1ab** | **802.3at** }

Parameters

Parameter	Description	Value
802.1ab	Indicates that the 802.3 Power via MDI TLV sent by the interface conforms to 802.1 ab.	-
802.3at	Indicates that the 802.3 Power via MDI TLV sent by the interface conforms to 802.3 at.	-

Views

Ethernet interface view, GE interface view, XGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 802.3 Power via MDI TLV has the following formats:

- 802.1 ab format: [TLV type | TLV information string length | 802.3 OUI | MDI power support | PSE power pair | power class]
- 802.3 at format: [TLV type | TLV information string length | 802.3 OUI | MDI power support | PSE power pair | power class | type/source/priority | PD requested power value | PSE allocated power value]

Based on 802.1 ab, 802.3 at extends three fields: type/source/priority, PD requested power value, and PSE allocated power value.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The LLDP function has been enabled globally and on interfaces.

Precautions

After the global LLDP is disabled, the LLDP configuration is deleted from all interfaces.

Before selecting a format of the 802.3 Power via MDI TLV, you must know the TLV format supported by the neighbors. The TLV format on the local device must be the same as that on the neighbors.

Member interfaces of the Eth-Trunk do not support this command.

Example

Configure the interface to send the 802.3 Power via MDI TLV conforming to 802.3 at.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] lldp dot3-tlv power 802.3at
```

Related Topics

21.6.1 display lldp local
21.6.10 lldp enable (system view)
21.6.9 lldp enable (interface view)

21.6.9 lldp enable (interface view)

Function

The **lldp enable** command enables LLDP on an interface.

The **undo lldp enable** command disables LLDP on an interface.

After LLDP is enabled in the system view, all interfaces are enabled with LLDP.

Format

lldp enable

undo lldp enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, port group view, Serial interface view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After LLDP is enabled on an interface, the interface exchanges LLDP packets with LLDP-enabled neighbors. The interface receives status information from the neighbors and sends the local status information to the neighbors. The NMS then obtains the status information for topology discovery.

Prerequisites

The LLDP function has been enabled globally.

Precautions

LLDP can be enabled in the system view and the interface view.

- After LLDP is enabled in the system view, all interfaces are enabled with LLDP.
- After LLDP is disabled in the system view, all LLDP settings are restored to the default settings except the setting of LLDP trap. Therefore, LLDP is also disabled on all interfaces.
- An interface can send and receive LLDP packets only after LLDP is enabled in both the system view and the interface view.
- After LLDP is disabled globally, the commands for enabling and disabling LLDP on an interface do not take effect.
- If LLDP needs to be disabled on some interfaces, enable LLDP globally first, and run the **undo lldp enable** command on these interfaces. To re-enable LLDP on these interfaces, run the **lldp enable** command in the views of these interfaces.

NOTE

- LLDP can be enabled and disabled only on the physical interfaces, but cannot be used on logical interfaces such as VLANIF interface and Eth-Trunk.
- On an Eth-Trunk, LLDP can only be enabled on member interfaces. The interfaces enabled with LLDP and not enabled with LLDP can exist in the same Eth-Trunk.
- Only serial interfaces enabled with PPP and HDLC support LLDP.

Example

Disable LLDP on Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] undo lldp enable
Info: The LLDP is disable on the port successfully.
```

Related Topics

21.6.1 display lldp local

21.6.10 lldp enable (system view)

 Copyright © Huawei Technologies Co., Ltd.

21.6.10 lldp enable (system view)

Function

The **lldp enable** command enables LLDP globally.

The **undo lldp enable** command disables LLDP globally.

By default, LLDP is disabled globally.

Format

lldp enable

undo lldp enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view the Layer 2 link status or analyze network topology, run the **lldp enable** command.

Configuration Impact

After LLDP is enabled globally, the device sends its own status information to LLDP-enabled neighbors and receives the status information from the neighbors.

Precautions

The interval between enabling LLDP globally and disabling LLDP cannot be shorter than 10 seconds; otherwise, an error message is displayed.

LLDP can be enabled in the system view and the interface view.

- After LLDP is enabled in the system view, all interfaces are enabled with LLDP.
- After LLDP is disabled in the system view, all LLDP settings are restored to the default settings except the setting of LLDP trap. Therefore, LLDP is also disabled on all interfaces.
- An interface can send and receive LLDP packets only after LLDP is enabled in both the system view and the interface view.
- After LLDP is disabled globally, the commands for enabling and disabling LLDP on an interface do not take effect.

Copyright © Huawei Technologies Co., Ltd.

Example

Enable LLDP globally.

```
<Huawei> system-view
[Huawei] lldp enable
Info: Global LLDP is enabled successfully.
```

Disable LLDP globally.

```
<Huawei> system-view
[Huawei] undo lldp enable
Warning: This command will delete the configurations of LLDP on all the ports.Continue?[Y/N]y
Info: Global LLDP is disabled successfully.
```

21.6.11 lldp management-address

Function

The **lldp management-address** command configures the LLDP management IP address.

The **undo lldp management-address** command restores the default setting.

By default, the system automatically obtains the management IP address.

Format

lldp management-address *ip-address*

undo lldp management-address

Parameters

Parameter	Description	Value
ip-address	Specifies the management IP address.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The management IP address is carried in the management address TLV field of the LLDP packet. It is used by the NMS to identify and manage devices. A management address identifies a device, facilitating the layout of the network topology and network management. To allocate a management address to a neighbor, run the **lldp management-address** command.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The LLDP function has been enabled globally.

The management IP address to be allocated must be a valid IP address existing on the device.

Configuration Impact

After the configuration, the management IP address is added to the management address TLV field of the LLDP packet. The NMS then identifies the device according to the management IP address.

Precautions

This command cannot be used to configure an IP address for an interface board.

If the configured management IP address is invalid or no management IP address is configured, the system sets an IP address in the address list as the management IP address. The system selects the IP address in the following sequence: loopback interface address, VLANIF interface address, and Layer 3 interface address. Among the IP addresses of the same type, the system selects the smallest one. If the system does not find a management IP address, the bridge MAC address is used as the management IP address.

Example

Set the LLDP management IP address to 10.10.10.1.

```
<Huawei> system-view
[Huawei] lldp management-address 10.10.10.1
```

Related Topics

21.6.1 display lldp local

21.6.10 lldp enable (system view)

21.6.12 lldp message-transmission delay

Function

The **lldp message-transmission delay** command sets the LLDP packet transmission delay.

The **undo lldp message-transmission delay** command restores the default LLDP packet transmission delay.

By default, the LLDP packet transmission delay is 2 seconds.

Format

lldp message-transmission delay *delay*

undo lldp message-transmission delay

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
delay	Specifies the LLDP packet transmission delay.	The value is an integer ranging from 1 to 8192, in seconds. The default value is 2 seconds. The *delay* value depends on the *interval* value in **lldp message-transmission interval**. The *delay* value must be equal to or smaller than a quarter of the *interval* value.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a delay before the interface sends an LLDP packet to the neighbor when the device status changes frequently. After the LLDP packet transmission delay is set on the device, the LLDP-enabled interfaces send LLDP packets to neighbors after a delay (the delay is the same as or longer than the delay you specified). The interfaces may send LLDP packets at different time points.

If the device status changes frequently, extend the delay in preventing the device from frequently sending packets to the neighbors. A delay suppresses the network topology flapping.

Prerequisites

The LLDP function has been enabled globally.

Configuration Impact

The LLDP packet transmission delay must be set properly and adjusted according to network loads.

- A large value reduces the LLDP packet transmission frequency when the local device status frequently changes. This helps save system resources. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.

 Copyright © Huawei Technologies Co., Ltd.

- A small value increases the LLDP packet transmission frequency and enables the NMS to discover network topology changes in real time when the local device status frequently changes. However, if the value is too small, LLDP packets are exchanged frequently, increasing the system load.
- The default value is recommended.

Precautions

Consider the value of *interval* when adjusting the value of *delay* because it is restricted by the value of *interval*.

- The value of *delay* ranges from 1 to 8192.
- The value of *delay* must be smaller than or equal to a quarter of *interval*. Therefore, if you want to set *delay* to be greater than a quarter of *interval*, first increase the *interval* value to four times the new *delay* value, and then increase the *delay* value.

NOTE

If the *interval* value is smaller than four times the *delay* value, the system displays an error message when you run the **undo lldp message-transmission delay** command. To run the **undo lldp message-transmission delay** command in this case, increase the *interval* value to at least four times the *delay* value first.

Example

Set the LLDP packet transmission delay to 5 second.

```
<Huawei> system-view
[Huawei] lldp message-transmission delay 5
```

Related Topics

21.6.1 display lldp local

21.6.10 lldp enable (system view)

21.6.14 lldp message-transmission interval

21.6.13 lldp message-transmission hold-multiplier

Function

The **lldp message-transmission hold-multiplier** command sets the hold time multiplier of device information stored on neighbors.

The **undo lldp message-transmission hold-multiplier** command restores the default hold time multiplier of device information stored on neighbors.

The default hold time multiplier is 4.

Format

lldp message-transmission hold-multiplier *hold*

undo lldp message-transmission hold-multiplier

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
hold	Specifies the hold time multiplier of device information on neighbors.	The value is an integer ranging from 2 to 10. The default value is 4.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The time multiplier is used to calculate how long a packet can be saved on a neighboring node. After receiving an LLDP packet, a neighbor updates the aging time of the device information from the sender based on the TTL.

The storage time calculation formula is: TTL = Min (65535, (*interval* x *hold*)).

TTL is the device information storage time. It is the smaller value between 65535 and (*interval* x *hold*).

interval indicates the interval at which the device sends LLDP packets to neighbors. This parameter is set by **lldp message-transmission interval**. *hold* indicates the hold time multiplier of device information on neighbors.

Prerequisites

The LLDP function has been enabled globally.

Configuration Impact

The hold time multiplier of device information on neighbors must be set to a proper value.

- A large value of *hold* prevents network topology flapping. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A small value of *hold* enables the NMS to discover topology change in time. However, if the value is too small, the neighbors update device information too frequently. This increases the load on the system and wastes resources.
- The default value is recommended.

Example

Set the hold time multiplier of device information on neighbors to 5.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] lldp message-transmission hold-multiplier 5
```

Related Topics

21.6.1 display lldp local

21.6.10 lldp enable (system view)

21.6.14 lldp message-transmission interval

21.6.14 lldp message-transmission interval

Function

The **lldp message-transmission interval** command sets the LLDP transmission interval.

The **undo lldp message-transmission interval** command restores the default LLDP transmission interval.

The default LLDP transmission interval is 30 seconds.

Format

lldp message-transmission interval *interval*

undo lldp message-transmission interval

Parameters

Parameter	Description	Value
interval	Specifies the LLDP transmission interval.	The value is an integer ranging from 5 to 32768, in seconds. The default value is 30 seconds. The *interval* value depends on the *delay* value in **lldp message-transmission delay**. The value of *interval* must be equal to or greater than four times the value of *delay*. Otherwise, an error occurs in the configuration.

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the LLDP status of the device keeps unchanged or the device does not discover new neighbors, the interface sends LLDP packets to the neighbors at a certain interval. After the LLDP transmission interval is set on the device, the LLDP enabled interfaces send LLDP packets to neighbors at this interval. The interfaces may send LLDP packets at different time points.

If you want to change the network topology detection frequency, run the **lldp message-transmission interval** command to change the LLDP transmission interval.

Prerequisites

The LLDP function has been enabled globally.

Configuration Impact

The LLDP transmission interval must be set properly and adjusted according to network loads.

- A large value reduces the LLDP packet transmission frequency. This helps save system resources. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A short interval increases the LLDP packet transmission frequency and enables the NMS to discover network topology changes in real time. However, if the interval is too short, LLDP packets are exchanged frequently, increasing the system load.
- The default value is recommended.

Precautions

Consider the value of *delay* when adjusting the value of *interval* because it is restricted by the value of *delay*.

- The value of *interval* ranges from 5 to 32768.
- The value of *interval* must be equal to or greater than four times the value of *delay*. Therefore, if you want to set *interval* to be smaller than four times the value of *delay*, first reduce the *delay* value to be equal to or smaller than a quarter of the new *interval* value, and then reduce the *interval* value.

NOTE

If the *delay* value is greater than a quarter of the *interval* value, the system displays an error message when you run the **undo lldp message-transmission interval** command. To run the **undo lldp message-transmission interval** command in this case, reduce the *delay* value to be equal to or smaller than a quarter of *interval* first.

Example

Set the LLDP transmission interval to 35 seconds.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] lldp message-transmission interval 35
```

Related Topics

21.6.1 display lldp local
21.6.10 lldp enable (system view)
21.6.12 lldp message-transmission delay

21.6.15 lldp restart-delay

Function

The **lldp restart-delay** command sets the delay in re-enabling the LLDP function on an interface.

The **undo lldp restart-delay** command restores the default delay in re-enabling the LLDP function on an interface.

The default delay is 2 seconds.

Format

lldp restart-delay *delay*

undo lldp restart-delay

Parameters

Parameter	Description	Value
delay	Specifies the delay in re-enabling the LLDP function on an interface.	The value is an integer ranging from 1 to 10, in seconds. The default value is 2 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a delay before LLDP is re-enabled on an interface. The delay suppresses the topology flapping caused by the frequent LLDP status changes.

Prerequisites

The LLDP function has been enabled globally.

Copyright © Huawei Technologies Co., Ltd.

Configuration Impact

The delay in re-enabling the LLDP function on an interface must be set properly.

- A large value of *delay* prevents network topology flapping. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A small value of *delay* enables the NMS to discover topology change in time. However, if the value is too small, the neighbors update device information too frequently. This increases the load on the system and wastes resources.
- The default value is recommended.

Example

Set the delay in re-enabling the LLDP function on an interface to 3 second.

```
<Huawei> system-view
[Huawei] lldp restart-delay 3
```

Related Topics

21.6.1 display lldp local

21.6.10 lldp enable (system view)

21.6.16 lldp tlv-enable

Function

The **lldp tlv-enable** command sets the type of the TLVs that can be sent by an interface.

The **undo lldp tlv-enable** command sets the type of the TLVs disabled on an interface.

By default, an interface advertises all types of TLVs except the Location Identification TLV.

Format

lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

lldp tlv-enable dot1-tlv { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **protocol-identity** }

lldp tlv-enable dot3-tlv { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** }

lldp tlv-enable med-tlv { **all** | **capability** | **inventory** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* } & <1-10> | **elin-address** *Tel-Number* } | **network-policy** | **power-over-ethernet** }

undo lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

Copyright © Huawei Technologies Co., Ltd.

undo lldp tlv-enable dot1-tlv { **all** | **port-vlan-id** | **protocol-vlan-id** | **vlan-name** | **protocol-identity** }

undo lldp tlv-enable dot3-tlv { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** }

undo lldp tlv-enable med-tlv { **all** | **capability** | **inventory** | **location-id** [**civic-address** | **elin-address**] | **network-policy** | **power-over-ethernet** }

Parameters

Parameter	Description	Value
all	• Indicates to advertise all types of TLVs when the device advertises basic TLVs, TLVs in the IEEE 802.1 format, and TLVs in the IEEE 802.3 format. • After the **all** parameter is specified, all MED TLVs except the Location Identification TLV are advertised.	-
basic-tlv	Indicates to advertise basic TLVs that include: • Management-address TLV • Port Description TLV • System Capabilities TLV • System Description TLV • System Name TLV	-
management-address	Indicates to advertise Management-address TLV.	-
port-description	Indicates to advertise Port Description TLV.	-
system-capability	Indicates to advertise System Capabilities TLV.	-
system-description	Indicates to advertise System Description TLV.	-
system-name	Indicates to advertise System Name TLV.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dot1-tlv	Indicates to advertise the TLVs in the IEEE 802.1 format that include: • Port VLAN TLV • Port protocol VLAN TLV • VLAN Name TLV • Protocol identity TLV **NOTE** Only Layer 2 physical interfaces such as Ethernet and GE interfaces support **dot1-tlv** and related parameters.	-
port-vlan-id	Indicates to advertise port VLAN TLV. The VLAN ID is the default VLAN ID on the interface.	-
protocol-vlan-id [*vlan-id*]	Indicates to advertise port protocol VLAN TLV. If *vlan-id* is not specified, the interface does not support protocol VLAN TLVs.	The value of *vlan-id* is an integer that ranges from 1 to 4094.
vlan-name [*vlan-id*]	Indicates to advertise VLAN Name TLV. If *vlan-id* is not specified, the default VLAN ID is used.	The value of *vlan-id* is an integer that ranges from 1 to 4094.
protocol-identity	Indicates to advertise protocol identity TLV.	-
dot3-tlv	Indicates to advertise the TLVs in the IEEE 802.3 format that include: • Link Aggregation TLV • MAC/PHY Configuration/Status TLV • Maximum Frame Size TLV • Power Via MDI TLV	-
link-aggregation	Indicates to advertise Link Aggregation TLV.	-
mac-physic	Indicates to advertise MAC/PHY Configuration/Status TLV.	-
max-frame-size	Indicates to advertise Maximum Frame Size TLV.	-
power	Indicates to advertise Power Via MDI TLV.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
med-tlv	Indicates to advertise MED TLVs that include: • LLDP-MED Capabilities TLV • Inventory TLV • Location Identification TLV • Network Policy TLV • Extended Power-via-MDI TLV	-
capability	Indicates to advertise MED Capabilities TLV.	-
inventory	Indicates to advertise Hardware Revision TLV, Firmware Revision TLV, Software Revision TLV, Serial Number TLV, Manufacturer Name TLV, Model Name TLV, and Asset ID TLV.	-
location-id	Indicates to advertise Location Identification TLV.	-
civic-address *device-type country-code* { *ca-type ca-value* } &<1-10>	Indicates to advertise the common address information of the network devices encapsulated in Location Identification TLV. • *device-type* specifies the type of the device. The value is an integer that ranges from 0 to 2. 0 indicates that the device is a DHCP server. 1 indicates that the device is a switch. 2 indicates that the device is an MED endpoint. • *country-code* specifies the country code. For the value range, see ISO 3166. • { *ca-type ca-value* }&<1-10> specifies the address information. *ca-type* specifies the type of address information. The value is an integer that ranges from 0 to 255. *ca-value* specifies the content of the address information. The value is a string of 1-250 characters. **<1-10>** indicates that the preceding parameters can be entered 10 times.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
elin-address *Tel-Number*	Advertises the emergency phone number encapsulated in Location Identification TLV.	The value is a string of 10 to 25 numerals. Each numeral ranges from 0 to 9.
network-policy	Advertises Network Policy TLV. Network Policy TLV is used to exchange VLAN configurations between network devices and terminal devices. A switch uses the TLV to advertise voice VLAN ID and voice stream priority to an IP phone. Then the IP phone forwards packets according to the received voice VLAN ID and priority, ensuring the voice quality.	-
power-over-ethernet	Advertises Extended Power via MDI TLV.	-

Views

Ethernet interface view, GE interface view, XGE interface view, port group view, Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In LLDP, all device information is encapsulated in Link Layer Discovery Protocol data units (LLDPDUs), which are then sent to neighbors. An LLDPDU contains a variety of TLVs. In a TLV, T indicates the information type, L indicates the information length, and V indicates the value or the content to be sent.

Devices exchange LLDPDUs carrying TLVs to obtain neighbor information. The TLVs that can be encapsulated in an LLDP packet include basic TLVs, TLVs in the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs.

Basic TLVs are essential for managing network devices. The TLVs in the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs are defined by standardization organizations and other organizations, which are used to enhance the network device management. You can determine whether to advertise the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs.

Devices on both ends can have different TLV types configured. You only need to configure TLV types according to networking requirements.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The LLDP function is enabled globally and on interfaces.

Precautions

- When the supported TLVs are basic TLVs, TLVs in the IEEE 802.1 format, and TLVs in the IEEE 802.3 format, the **lldp tlv-enable** command with the **all** parameter advertises all TLVs. When the supported TLVs are MED TLVs, the **lldp tlv-enable** command with the **all** parameter advertises all TLVs except Location Identification TLV.

  If the **all** parameter is not specified, only one type of TLV can be advertised. To advertise multiple types of TLVs, run this command multiple times.
- You can specify the other types of MED TLVs only after specifying the MED Capabilities TLV.

  To disable the MED Capabilities TLV, first disable the other types of MED TLVs.

  To disable the MAC/PHY Configuration/Status TLVs, first disable the MED Capabilities TLV.
- The 802.3 MAC/PHY Configuration/Status TLVs are automatically advertised after the MED Capabilities TLV is advertised.
- If you disable the MED TLVs using the command with the **all** parameter, the 802.3 MAC/PHY Configuration/Status TLVs are not disabled automatically.
- A serial interface can advertise only basic TLVs.

Example

Configure Ethernet2/0/0 to advertise the Link Aggregation TLV in the IEEE 802.3 format.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] lldp tlv-enable dot3-tlv link-aggregation
```

Related Topics

21.6.10 lldp enable (system view)

21.6.5 display lldp tlv-config

21.6.17 lldp tlv-enable private-tlv authentication

Function

The **lldp tlv-enable private-tlv authentication** command enables LLDP packet authentication.

The **undo lldp tlv-enable private-tlv authentication** command disables LLDP packet authentication.

By default, LLDP packet authentication is disabled.

Format

lldp tlv-enable private-tlv authentication password { **simple** | **cipher** } *password*

Copyright © Huawei Technologies Co., Ltd.

undo lldp tlv-enable private-tlv authentication

Parameters

Value	Description	Value
simple	Indicates the password in plain text. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
cipher	Indicates the password in cipher text. The password is displayed in cipher text.	-
password	Specifies the password for LLDP packet authentication.	The value is a string of case-sensitive characters without command line characters such as spaces and question marks (?). • When **simple** is specified, the password is in plaintext and contains 1 to 32 characters. • When **cipher** is specified, the password can be either in ciphertext or plaintext, depending on what is entered. The password in plaintext contains 1 to 32 characters, such as **huawei123**. The password in ciphertext must be a string of 48 characters, for example, **%^%#/}pb(9>!)4@plQ<Z]@UG2WH45|y/DE=%p<5K,ZJU%^%#**.

Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, GE interface view, XGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the **lldp tlv-enable private-tlv authentication** command is run an interface, the interface is blocked immediately and can be connected only when the password in LLDP packets sent from the peer end is the same as that configured on the interface.

Prerequisites

The LLDP function has been enabled globally.

Precaution

This command only supports configuration on Layer 2 interface.

Example

Enable LLDP packet authentication on Ethernet2/0/0 and set the password in plaintext to **huawei123**.

```
<Huawei> system-view
[Huawei] interface Ethernet 2/0/0
[Huawei-Ethernet2/0/0] lldp tlv-enable private-tlv authentication password simple huawei123
```

Related Topics

21.6.10 lldp enable (system view)

21.6.18 lldp trap-interval

Function

The **lldp trap-interval** command sets the delay in sending neighbor change traps to the NMS.

The **undo lldp trap-interval** command restores the default delay in sending neighbor change traps to the NMS.

By default, the device sends a neighbor change trap to the NMS after a 5-second delay.

Format

lldp trap-interval *interval*

undo lldp trap-interval

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the delay in sending traps.	The value is an integer ranging from 5 to 3600, in seconds. The default value is 5 seconds. The default value is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a delay before the device sends LLDP traps about neighbor information changes to the NMS. When neighbor information changes frequently, you can prolong the delay. In this way, the device will not frequently send traps to the NMS, and the network topology flapping is suppressed.

Prerequisites

The LLDP function has been enabled globally.

Configuration Impact

After the delay is set on the device, LLDP-enabled interfaces send LLDP traps to neighbors after a delay (the delay is the same as or longer than the delay you specified). The interfaces may send LLDP traps at different time points.

Precautions

The configured delay applies only to the trap, which reports changes in neighbor information, including the number of added neighbors, number of deleted neighbors, number of neighbors that are aged out, and number of neighbors of which the information is deleted.

Example

Set the delay in sending neighbor change traps to 6 seconds.

```
<Huawei> system-view
[Huawei] lldp trap-interval 6
```

Related Topics

21.6.1 display lldp local

Copyright © Huawei Technologies Co., Ltd.

21.6.10 lldp enable (system view)

21.6.19 reset lldp statistics

Function

The **reset lldp statistics** command clears LLDP packet statistics on all interfaces or on a specified interface.

Format

reset lldp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the interface where the LLDP statistics you want to reset. In the command: • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If no interface is specified, LLDP packet statistics of all interfaces are cleared.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To troubleshoot LLDP faults, you may need to view LLDP packet statistics within a certain period of time. In this case, you must run the **reset lldp statistics** command to clear existing LLDP packet statistics, and run the **display lldp statistics** command to view the new LLDP packet statistics.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The LLDP function has been enabled globally and on interfaces.

Example

Clear LLDP packet statistics on all interfaces.

```
<Huawei> reset lldp statistics
Warning: This Command will clear LLDP statistics of all the ports. Continue? [Y/N]:y
```

Clear LLDP packet statistics of Ethernet2/0/0.

```
<Huawei> reset lldp statistics interface ethernet 2/0/0
```

Related Topics

21.6.4 display lldp statistics

21.6.10 lldp enable (system view)

21.6.20 snmp-agent trap enable feature-name lldptrap

Function

The **snmp-agent trap enable feature-name lldptrap** command enables the LLDP trap function on the device.

The **undo snmp-agent trap enable feature-name lldptrap** command disables the LLDP trap function on the device.

By default, the LLDP trap function is enabled.

Format

snmp-agent trap enable feature-name lldptrap [**trap-name** { **hwlldpdisabled** | **hwlldpenabled** | **hwlldplocmanipaddrchange** | **lldpremtableschange** }]

undo snmp-agent trap enable feature-name lldptrap [**trap-name** { **hwlldpdisabled** | **hwlldpenabled** | **hwlldplocmanipaddrchange** | **lldpremtableschange** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event.	-
hwlldpdisabled	Sends a Huawei proprietary trap when the LLDP function is disabled globally.	-
hwlldpenabled	Sends a Huawei proprietary trap when the LLDP function is enabled globally.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwlldplocmanipaddrch-ange	Sends a Huawei proprietary trap when the LLDP management address of the device changes.	-
lldpremtableschange	Sends a trap when LLDP neighbor information changes.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device to send traps when the LLDP status changes, run the **snmp-agent trap enable feature-name lldptrap** command.

Prerequisites

A reachable route exists between the device and the NMS, and the SNMP parameters are set.

Configuration Impact

After the LLDP trap function is enabled, the device sends traps to the NMS in one of the following cases:

- The LLDP function is enabled or disabled globally.
- The local management address changes.
- A neighbor is added, deleted, discarded, or aged out.

Precautions

The LLDP trap function applies to all interfaces.

If the network topology is unstable, disable the LLDP trap function to prevent frequent trap sending.

To set the interval between sending neighbor change traps to the NMS, run the **lldp trap-interval** command. If neighbor information changes frequently, extend the interval to reduce the number of traps.

Example

Enable the LLDP trap function on the device.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name lldptrap
```

Related Topics

21.6.6 display snmp-agent trap feature-name lldptrap all

21.7 NQA Configuration Commands

21.7.1 adv-factor

Function

The **adv-factor** command configures an advantage factor for simulated voice calculation in an NQA jitter test.

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

By default, the advantage factor for simulated voice test calculation is 0.

Format

adv-factor *factor-value*

undo adv-factor

Parameters

Parameter	Description	Value
factor-value	Specifies the advantage factor for simulated voice test calculation.	The value is an integer that ranges from 0 to 20. The default value is 0.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network bearing VoIP services, a jitter test is used to test VoIP service quality. The **adv-factor** command is used to configure the advantage factor for voice test calculation to simulate packet jitter generated by actual voice packets.

When calculating the quality parameter R value of the voice transmission network, a test engineer needs to specify an advantage factor according to the transmission distance and media. The value shows the expected compensation for voice quality

Copyright © Huawei Technologies Co., Ltd.

degradation during network transmission. The user-defined value is determined by the type of the network to be tested. The higher the expected level of service quality degradation, the greater the value. The *factor-value* parameter shows tolerance over a certain level of voice quality degradation during network transmission.

For example:

- Set the advantage factor to 0 in testing a common wire communication system.
- Set the advantage factor to 20 in testing a multi-hop FR network connected to the satellite.

Prerequisites

The **adv-factor** command can be used only after the following conditions are met:

- The UDP jitter test is used.
- The code type for the simulated voice test of a jitter test instance has been set using the **jitter-codec** command. The code types of g711a, g711u, and g729a are applied to the VoIP applications of conversion between simulated voice signals and digital signals.
- The **nqa-server udpecho** command has been run on the remote device to respond to the jitter test.

Configuration Impact

If the advantage factor has been configured, running the **adv-factor** command will override the previous configuration.

If the code type is changed after the **jitter-codec** command is run, the configured advantage factor does not take effect and you need to configure a new advantage factor.

Precautions

The advantage factor of a running test instance cannot be changed.

Example

Set the advantage factor for a simulated voice test calculation to 20.

```
<Huawei> system-view
[Huawei] nqa test-instance admin jitter
[Huawei-nqa-admin-jitter] test-type jitter
[Huawei-nqa-admin-jitter] jitter-codec g711a
[Huawei-nqa-admin-jitter] adv-factor 20
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.46 jitter-codec

Copyright © Huawei Technologies Co., Ltd.

21.7.2 agetime

Function

The **agetime** command sets the aging time of an NQA test instance.

The **undo agetime** command restores the default aging time of an NQA test instance.

The default aging time of an NQA test instance is 0, indicating that the test instance is not aged.

Format

agetime *hh:mm:ss*

undo agetime

Parameters

Parameter	Description	Value
hh:mm:ss	Specifies the aging time.	*hh* ranges from 0 to 23; *mm* ranges from 0 to 59; *ss* ranges from 0 to 59.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent endless running of a test instance, you need to age the test instance periodically. The **agetime** command can be used to configure the aging time to change the survival time of a test instance in the system.

- The aging time is started when the NQA test instance is in the inactive state. When the aging time expires, the system deletes the NQA test instance automatically.
- The aging time is reset when the NQA test instance is in the active state.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Precautions

The aging time of a running test instance cannot be changed.

Copyright © Huawei Technologies Co., Ltd.

Example

Set the aging time of NQA test instance **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] agetime 1:0:0
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.3 alarm

Function

The **alarm** command sets an alarm threshold for the monitored item of an NQA test result.

The **undo alarm** command deletes an alarm threshold for the monitored item of an NQA test result.

By default, no alarm threshold is configured for the monitored item of an NQA test result.

Format

alarm *entry-number* { **jitter-average** | **jitter-ds-average** | **jitter-sd-average** | **lost-packet-ratio** | **packet-loss-ds** | **packet-loss-sd** | **rtt-average** } { **absolute** | **delta** } { **falling-threshold** *threshold-value1 event-entry1* | **rising-threshold** *threshold-value2 event-entry2* } * [**description** *description*]

undo alarm [*entry-number*]

Parameters

Parameter	Description	Value
entry-number	Specifies the index of an entry.	The value is an integer that ranges from 1 to 65535.
jitter-average	Indicates the average jitter value. This value is available only for jitter test instances.	-
jitter-ds-average	Indicates the average jitter value of packets from the destination to the source. This value is available only for jitter test instances.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
jitter-sd-average	Indicates the average jitter value of packets from the source to the destination. This value is available only for jitter test instances.	-
lost-packet-ratio	Indicates the packet loss ratio. This value is available for all test instances.	-
packet-loss-ds	Indicates the number of lost packets sent from the destination to the source. This value is available only for jitter test instances.	-
packet-loss-sd	Indicates the number of lost packets sent from the source to the destination. This value is available only for jitter test instances.	-
rtt-average	Indicates the average round trip time (RTT). This value is available for all test instances.	-
absolute	Indicates an absolute sampled value, which refers to the sampled value obtained this time.	-
delta	Indicates a relative sampled value, which refers to a changed value comparing with the last sampled value	-
falling-threshold *threshold-value1*	Specifies the lower threshold.	The value is an integer that ranges from 0 to 2147483647.
event-entry1	Specifies the index of the entry corresponding to the lower threshold in the event table.	The value is an integer that ranges from 1 to 65535.
rising-threshold *threshold-value2*	Specifies the upper threshold.	The value is an integer that ranges from 0 to 2147483647.
event-entry2	Specifies the index of the entry corresponding to the upper threshold in the event table.	The value is an integer that ranges from 1 to 65535.
description	Indicates the description of this alarm.	The value is a string of 1 to 127 case-sensitive characters with spaces supported.

Views

NQA view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the monitored item of an NQA test result exceeds the threshold, the system sends an alarm to the NMS.

According to the NQA alarm mechanism, an alarm is generated when the monitored item exceeds the threshold only after an alarm threshold and an alarm event are both configured. The system will generate an alarm if the monitored item exceeds the upper or lower threshold configured in the event table. If an incorrect alarm variable is specified, for example, an inexistent OID is specified, no alarm will be generated.

You can run the **alarm** command to add or delete an alarm entry in the NQA alarm table. If an alarm variable is specified, an alarm is generated when the system becomes abnormal. If the monitored item exceeds the threshold, an alarm is generated.

Prerequisites

An event has been associated with the NQA alarm using the **nqa event** command. An alarm table is determined by an event table. The entry number in an event table and the event number specified by an alarm must be consistent. Otherwise, if you run the **alarm** command, the system will display a message indicating that the alarm event does not exist.

The trap function has been enabled for the NQA module using the **snmp-agent trap enable feature-name nqa** command and the route between the device and NMS is reachable. In this way, NQA alarms can be sent to the network management system (NMS).

Configuration Impact

Ensure that the alarm entry to be entered is unique. If an alarm entry number exists and you enter the same entry number, the new entry number will override the configuration to which the original alarm corresponds.

Example

Configure alarms to be sent when the packet loss ratio exceeds the threshold.

```
<Huawei> system-view
[Huawei] nqa event 10 trap
[Huawei] nqa event 100 trap
[Huawei] nqa test-instance admin jitter
[Huawei-nqa-admin-jitter] test-type jitter
[Huawei-nqa-admin-jitter] alarm 10 lost-packet-ratio absolute falling-threshold 10 10 rising-threshold 100 100
```

Related Topics

21.7.58 nqa event

21.7.56 nqa

Copyright © Huawei Technologies Co., Ltd.

21.7.4 clear-records

Function

The **clear-records** command clears statistics on NQA test instances.

Format

clear-records

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Clearing statistics on the ongoing test is forbidden.

Before running the command, ensure that the test type specified by the **test-type** command exists.

Example

Clear all statistics on NQA test instance **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] clear-records
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.18 display nqa history

21.7.20 display nqa results

21.7.5 community read cipher

Function

The **community read cipher** command configures the community name for SNMP test.

The **undo community** command deletes the community name of SNMP test.

Copyright © Huawei Technologies Co., Ltd.

By default, the community name for SNMP test is public.

Format

community read cipher *community-name*

undo community

Parameters

Parameter	Description	Value
community-name	Specifies the community name for SNMP test.	The value is a string of case-sensitive characters without command line characters such as spaces and question marks. The length ranges from 1 to 32 for plain text and ranges from 32 to 68 for cipher text. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A community, uniquely identified by a community name, defines administrative relationships between NMSs and SNMP agents. The community name acts like a password to regulate access to an SNMP agent. An NMS can access an SNMP agent only if the community name carried in the SNMP request sent by the NMS is the same as the community name configured on the SNMP agent.

When the SNMP versions on agents are SNMPv1 or SNMPv2c, the community name must be configured using the **community read cipher** command, and the community name must be a read-only community name on SNMP agents. When the SNMP versions on agents are SNMPv3, the community name does not need to be configured because SNMPv3 does not support community names.

Prerequisites

The NQA test instance has been configured using the **nqa** command, and the test instance type has been set to SNMP using the **test-type** command.

Example

Set the community name for SNMP test.

```
<Huawei> system-view
[Huawei] nqa test-instance user test1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-nqa-user-test1] test-type snmp
[Huawei-nqa-user-test1] community read cipher Huawei-123
```

21.7.6 datafill

Function

The **datafill** command configures pad characters in an NQA test instance.

The **undo datafill** command deletes the pad characters in an NQA test instance.

By default, there are no padding characters in an NQA test instance.

Format

datafill *fillstring*

undo datafill

Parameters

Parameter	Description	Value
fillstring	Specifies the pad characters for NQA test packets.	The value is a string of 1 to 230 case-sensitive characters with spaces supported. The question mark (?) is not supported. The default value is 0 (an empty pad character).

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an NQA test, you need to simulate actual datagrams to obtain more accurate statistics. The **datasize** command can be used to set the size of the Data field. To differentiate packets sent from different test instances, add the specified characters to identify the test packets.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The type can be one of the following:

- UDP
- Jitter
- ICMP

Copyright © Huawei Technologies Co., Ltd.

- Trace
- LSP Ping

Configuration Impact

After the **datafill** command is run, the following situations may occur:

- If the length of the data packet sent from the test instance is shorter than the configured pad character, only the forepart of the pad character can be used.
- If the length of the data packet sent from the test instance is larger than the configured pad character, the pad character is repeated in sequence until the data packet is successfully padded.

For example, the pad character is set to **abcd**. If the length of the test packet is 3, only **abc** is used to pad the test packet. If the length of the test packet is 6, **abcdab** is used to pad the test packet.

Precautions

The pad character of a running test instance cannot be changed.

Example

Set the pad characters of the test named **user test** to **abcd**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] datafill abcd
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.7 datasize

21.7.7 datasize

Function

The **datasize** command sets the size of the NQA test packet.

The **undo datasize** command restores the size of the NQA test packet.

The default size is 0, which indicates that the test packet does not carry data information.

Format

datasize *size*

undo datasize

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
size	Specifies the size of the NQA test packet.	The value is an integer that ranges from 0 to 8100, in bytes. If the configured size of a packet is smaller than the default size of a packet, the configured size is invalid and the packet is forwarded based on its default size. **NOTE** When you run the **hardware-based enable** command for a Jitter test instance, the value ranges from 0 to 1472, in bytes.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **datasize** command to set the size of the data field of a test packet. This ensures that the size of the test packet is closer to the size of the actual data packet and the obtained statistics are more accurate.

For example, if a UDP jitter test instance is used to detect voice over IP (VoIP) services, you can run the **datasize** command to set the size of the NQA test packet to the same size as the actual voice packet. This enables a simulation of the actual traffic that occurs in a period of time.

To simulate a voice data flow with the transmission rate of 64 kbit/s, you can set the size of the voice packet to 172 bytes (160-byte payload + 12-byte RTP header + 28-byte IP header and UDP header) and set the interval for sending the voice packet to 20 ms. In this manner, 3000 packets can be sent in one minute.

Prerequisites

The test type has been specified using the **test-type** command.

The **datasize** command is applicable only to the ICMP, UDP, trace, LSP ping, and jitter test instances.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

You cannot change the size of the running test packets.

Example

Set the size of the packets to 100 bytes in the test instance named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] datasize 100
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.41 interval (NQA view)

21.7.6 datafill

21.7.8 description (NQA view)

Function

The **description** command configures description of an NQA test instance.

The **undo description** command deletes the description of an NQA test instance.

By default, no description is configured for an NQA test instance.

Format

description *string*

undo description

Parameters

Parameter	Description	Value
string	Specifies the description of an NQA test instance.	The value is a string of 1 to 230 case-sensitive characters with spaces.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Copyright © Huawei Technologies Co., Ltd.

The **description** command can be used to briefly describe the test instance to help maintenance. Generally, the test item or the test objective of a test instance is described.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Configuration Impact

If the description of a test instance has been configured, running the **description** command will override the previous configuration.

Precautions

The description of a running test instance cannot be changed.

Example

Set the description of the test named **user test** to fortest.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] description fortest
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.9 destination-address

Function

The **destination-address** command specifies the destination address of an NQA test instance.

The **undo destination-address** command deletes the destination address of an NQA test instance.

By default, destination address is not configured for an NQA test instance.

Format

destination-address { **ipv4** *ipv4-address* [**lsp-masklen** *masklen* [**lsp-loopback** *loopback-address*] [**vpn-frr-path**] | **lsp-loopback** *loopback-address* [**lsp-masklen** *masklen*] [**vpn-frr-path**] | **vpn-frr-path**] | **ipv6** *ipv6-address* | **url** *urlstring* }

destination-address mac *mac-address*

undo destination-address

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv4 *ipv4-address*	Specifies an IPv4 destination address.	The IPv4 address is in dotted decimal notation.
lsp-masklen *masklen*	Specifies the mask length of an LSP's IPv4 address prefix.	The value is an integer that ranges from 0 to 32.
lsp-loopback *loopback-address*	Specifies a 127/8 IP address in the MPLS echo request packet header.	-
vpn-frr-path	Indicates that the connectivity of the backup VPN FRR LSP will be checked.	-
ipv6 *ipv6-address*	Specifies an IPv6 destination address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
url *urlstring*	Specifies a destination URL address.	The value is a string of 1 to 230 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
mac *mac-address*	Indicates the unicast MAC address.	A MAC address in the format of H-H-H. Each H stands for one to four hexadecimal characters.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **destination-address** command to specify the destination address of an NQA test instance.

Precautions

- The Label Switched Path (LSP) parameters can be configured only for the LSP test instances.
- You cannot configure destination IP address for DHCP test instances.
- You can specify the destination address as a URL address only for the HTTP, trace, and DNS test instances.

 Copyright © Huawei Technologies Co., Ltd.

- The destination addresses of DNS test instances must be URL addresses but cannot be IPv4 addresses, and the destination URL addresses must contain dots (.); otherwise, the test may fail.
- You cannot change the destination address of a running test instance.

Example

Configure the destination address for test instance **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] destination-address ipv4 10.1.1.1
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.10 destination-port

Function

The **destination-port** command configures the destination port number for an NQA test.

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

By default, no destination port number is specified for an NQA test.

Format

destination-port *port-number*

undo destination-port

Parameters

Parameter	Description	Value
port-number	Specifies the destination port number.	The value is integer that ranges from 1 to 65535. The configured port cannot be a well-known port or used by other modules.

Views

NQA view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to only the FTP, HTTP, Jitter, TCP, UDP, and Trace test instances.

Precautions

You cannot change the destination port number of the test that is being performed.

Example

Set the destination port number to 2020 for the test instance named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] destination-port 2020
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.11 display ip nqa-compatible responder statistics

Function

The **display ip nqa-compatible responder statistics** command displays statistics on the NQA handshake packets sent from the third-party device or NMS software.

Format

display ip nqa-compatible responder statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When a device works with a third-party device or NMS software to perform UDP-Echo or UDP-Jitter packets, this command displays statistics about NQA handshake packets sent from the third-party device or NMS software.

Prerequisites

The device is configured to respond to the UDP tests initiated by the third-party device or NMS software.

Example

Display statistics on NQA handshake packets sent from the third-party device or NMS software.

```
<Huawei> display ip nqa-compatible responder statistics
IP NQA-COMPATIBLEs Responder is: Enabled
Number of control message received:4
Recent success sources:
Number of successes:2
SIP            DIP            Sport  Dport  Tos  Time
------------------------------------------------------------------------------
10.10.10.26    10.10.10.14    30000  40000  36   [21:13:02.028 UTC 20 06 2013]
10.10.10.26    10.10.10.14    30000  40000  36   [21:13:12.008 UTC 20 06 2013]
Recent fail sources:
Fail reason: IP,PortNum or Tos matching failure.
Number of failures:2
SIP            DIP            Sport  Dport  Tos  Time
------------------------------------------------------------------------------
10.10.10.28    10.10.10.14    30001  40001  38   [21:13:06.358 UTC 20 06 2013]
10.10.10.28    10.10.10.14    30001  40001  38   [21:13:11.368 UTC 20 06 2013]
```

Table 21-40 Description of the display ip nqa-compatible responder statistics command output

Item	Description
IP NQA-COMPATIBLEs Responder is	Whether the device is enabled to respond to UDP-Echo or UDP-Jitter packets sent by the third-party device or NMS software.
Number of control message received	Number of received handshake packets.
Recent success sources	The third-party packets that are successfully received.
Number of successes	Number of packets that are successfully received.
SIP	Source IP address of packets.
DIP	Destination IP address of packets.
Sport	Source port of packets.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dport	Destination port of packets.
Tos	Packet priority.
Time	Packet receiving time.
Recent fail sources	The third-party packets that are failed to be received.
Fail reason	Reason of packet receiving failure.
Number of failures	Number of packets that are failed to be received.

21.7.12 display nqa application

Function

The **display nqa application** command displays the type of the NQA test instance that corresponds to the service.

Format

display nqa application

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You need to choose a proper NQA test instance type based on the service to be tested. You can run the **display nqa application** command to view the type of the NQA test instance that corresponds to the service.

NOTE

You can run this command to view the type of the NQA test instance corresponding to the service. However, the test instance that can be configured on the device uses the test instanced configured in the **test-type** command as an example.

Copyright © Huawei Technologies Co., Ltd.

Example

Display the type of the NQA test instance corresponding to the service.

```
<Huawei> display nqa application
Application: The area that you test.
Subclasss  : The subclass of application.
NQA type   : The type of NQA test-instance.
Application              Subclass                NQA type
------------------------------------------------------------------------------
internet                 ---                       http
                                                   ftp
                                                   dns
                                                   dhcp

streaming media          ---                     jitter

network performance      ---                     jitter

trouble-shooting         application               http
                                                   ftp
                                                   dns
                                                   dhcp
                                                   snmp

                         network                   udp
                                                   tcp
                                                   icmp
                                                   trace

                         link

                         mpls                    lspping
                                                 lsptrace
```

Table 21-41 Description of the display nqa application command output

Item	Description
Application	Service type.
Subclasss	Service sub-type.
NQA type	Type of the corresponding NQA test instance.

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.13 display nqa alarm

Function

The **display nqa alarm** command displays alarms of an NQA test instance.

Format

display nqa alarm [**test-instance** *admin-name test-name*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
test-instance *admin-name*	Specifies the administrator of an NQA test instance.	The value is a string of 1 to 32 characters.
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display nqa alarm** command to display current alarms of a specified test instance or all test instances.

NOTE

To display alarms of a single test instance, ensure that the specified test instance exists.

Example

Display alarms of a single NQA test instance.

```
<Huawei> display nqa alarm test-instance admin jitter
NQA Alarm Information:
------------------------------------------------------------------------
Admin-Name   Operation-Tag   Alarm-Entry   AlarmType   Event-Entry
------------------------------------------------------------------------
admin        jitter          10            Rising      10
admin        jitter          10            Falling     10
```

Table 21-42 Description of the display nqa alarm test-instance admin jitter command output

Item	Description
Admin-Name	Administrator of an NQA test instance.
Operation-Tag	Name of the test instance.
Alarm-Entry	Alarm number.
AlarmType	Alarm type.
Event-Entry	Associated event number.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.3 alarm

21.7.14 display nqa-alarm

Function

The **display nqa-alarm** command displays the maximum number of NQA alarms that the system allows and the number of current NQA alarms.

Format

display nqa-alarm

Parameters

None

Views

NQA view

Default Level

1: Monitoring level

Usage Guidelines

After you run the **display nqa-alarm** command, the maximum number of NQA alarms that the system allows and the number of current NQA alarms are displayed.

Example

Display the number of NQA alarms.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] display nqa-alarm
NQA alarm information:
------------------------------------------------------
NQA Alarm Max: 5              NQA Alarm Number: 0
------------------------------------------------------
```

Table 21-43 Description of the display nqa-alarm command output

Item	Description
NQA Alarm Max	Maximum number of NQA alarms that the system allows.
NQA Alarm Number	Number of current NQA alarms.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.56 nqa

21.7.3 alarm

21.7.15 display nqa event

Function

The **display nqa event** command displays the event associated with the alarm.

Format

display nqa event [*event-entry*]

Parameters

Parameter	Description	Value
event-entry	Specifies the index of the entry that is associated with the alarm in the event table. If this parameter is not specified, all events associated with alarms are displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display nqa event** command to view the event associated with the NQA alarm.

Example

Display event 10.

```
<Huawei> display nqa event 10
NQA Event Information:
------------------------------------------------------------------------------
Event-Entry     Event-type      Description     Admin-Name      Operation-Tag
------------------------------------------------------------------------------
10              linkage         None            admin           icmp
```

Table 21-44 Description of the display nqa event command output

Item	Description
Event-Entry	Number of the entry in the event table.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Event-type	Event type.
Description	Event description.
Admin-Name	Name of the administrator.
Operation-Tag	Name of linkage test instance.

Related Topics

21.7.58 nqa event

21.7.16 display nqa-event

Function

The **display nqa-event** command displays the maximum number of NQA events that the system allows and the number of configured NQA events.

Format

display nqa-event

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display nqa-event** command displays the maximum number of NQA events that the system allows and the number of NQA events that have been configured.

Example

Display information about NQA events.

```
<Huawei> display nqa-event
NQA event information:
------------------------------------------------------
NQA Event Max: 100              NQA Event Number: 0
------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 21-45 Description of the display nqa-event command output

Item	Description
NQA Event Max	Maximum number of NQA events that the system allows.
NQA Event Number	Number of configured NQA events.

Related Topics

21.7.58 nqa event

21.7.17 display nqa-group

Function

The **display nqa-group** command displays NQA group status.

Format

display nqa-group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Specifies the name of an NQA group.	The value is a string of 1 to 32 case-sensitive characters without spaces or question marks. If the character string is quoted by double quotation marks, the character string can contain spaces and question marks.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view NQA group status, run the **display nqa-group** command. By viewing NQA group status, you can know whether the probe of an NQA group is successful and the probe result of each NQA test instance, facilitating fault location.

If the *group-name* parameter is not specified, status of all NQA groups is displayed.

Copyright © Huawei Technologies Co., Ltd.

Example

View NQA group status.

```
<Huawei> display nqa-group
NQA-group information:
------------------------------------------------------------------------------
 NQA-group group1
     Admin-name                 Test-name                  State
 NQA  admin1                    test1                      NA
 NQA  admin2                    test2                      NA
 NQA  admin3                    test3                      NA
 NQA-group group2
     Admin-name                 Test-name                  State
 NQA  admin4                    test4                      NA
 NQA  admin5                    test5                      NA
------------------------------------------------------------------------------
```

Table 21-46 Description of the **display nqa-group** command output

Item	Description
NQA-group	Name of an NQA group.
Admin-name	Administrator of an NQA test instance.
Test-name	Name of an NQA test instance.
State	NQA group status: • UP: The probe of the NQA test instance is successful. • DOWN: The probe of the NQA test instance fails. • NA: The NQA test instance does not exist or the NQA test instance type is not ICMP. The probe of an NQA group is considered to be successful as long as the probe of one NQA test instance in the group is successful. If the probes of all NQA test instances fail, the probe of the NQA group fails.
NQA	NQA test instance information, including the administrator, name, and status of an NQA test instance.

Related Topics

21.7.69 nqa-group
21.7.57 nqa (NQA group view)

21.7.18 display nqa history

Function

The **display nqa history** command displays the history records about an NQA test.

 Copyright © Huawei Technologies Co., Ltd.

Format

display nqa history [**test-instance** *admin-name test-name*] [**from** *start-date start-time* **to** *end-date end-time*]

Parameters

Parameter	Description	Value
test-instance	Indicates NQA test instances.	-
admin-name	Specifies the name of the administrator for an NQA test instance.	It is a string of 1 to 32 characters, spaces not supported. When quotation marks are used around the string, spaces are allowed in the string.
test-name	Specifies the name of an NQA test instance.	It is a string of 1 to 32 characters, spaces not supported. When quotation marks are used around the string, spaces are allowed in the string.
start-date	Specifies the start date, in the format of YYYY/MM/DD.	YYYY specifies a year that ranges from 2000 to 2099; MM specifies a month that ranges from 1 to 12; DD specifies a day that ranges from 1 to 31.
start-time	Specifies the start time, in the format of HH:MM:SS.	HH specifies an hour that ranges from 0 to 23; MM specifies a minute that ranges from 0 to 59; SS specifies a second that ranges from 0 to 59.
end-date	Specifies the end date, in the format of YYYY/MM/DD.	YYYY specifies a year that ranges from 2000 to 2099; MM specifies a month that ranges from 1 to 12; DD specifies a day that ranges from 1 to 31.
end-time	Specifies the end time, in the format of HH:MM:SS.	HH specifies an hour that ranges from 0 to 23; MM specifies a minute that ranges from 0 to 59; SS specifies a second that ranges from 0 to 59.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

NQA provides NQA test instances to test network operation conditions, to export statistics, and to effectively cut costs. NQA measures the performance of different protocols running on the network.

The **display nqa history** command helps you understand the network status by displaying the operation statistics about each test packet, including the status and round-trip delay.

NOTE

No history record about the failed jitter test instances exist.

To filter out information about failed tests in a historical table related to ICMP test instances, run the **records history-filter** **failures** command before viewing historical statistics.

Precautions

If no optional parameter is specified, all history records of an NQA test instance are displayed.

When NQA test result table and historical table are displayed in a split screen, latest results are displayed to improve user experience.

Example

Display the history records about an NQA test.

```
<Huawei> display nqa history
 NQA entry(admin, ftp) history:
 Index  T/H/P     Response Status       Address       Time
 1      1/1/1     1157ms   success      10.2.1.2      2012-07-15 10:16:38.188
 2      2/1/1     3000ms   timeout      UnKnow        2012-07-15 10:18:2.922
 NQA entry(admin, http) history:
 Index  T/H/P     Response Status       Address       Time
 1      1/1/1     0ms      busy         UnKnow        2012-07-15 11:16:39.915
 2      1/1/2     0ms      busy         UnKnow        2012-07-15 11:16:39.978
 3      1/1/3     0ms      busy         UnKnow        2012-07-15 11:16:39.40
```

Table 21-47 Description of the display nqa history command output

Item	Description
NQA entry(admin, ftp)	NQA test items: • admin: indicates the name of the administrator for an NQA test instance. • ftp: indicates the name of the NQA test instance.
Index	Index of a test record.
T/H/P	• T: Times, which indicates the sequence of the test for a test instance. • H: Hop, which indicates the sequence of the hop. • P: Probe, which indicates the sequence of the probe.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Response	Period from the time when a probe packet is sent to the time when a response packet is received.
Status	Probe status: • success: indicates that the probe succeeds. • timeout: indicates that the probe times out and no response packet is received. • busy: indicates that the resources are insufficient and the probe packet fails to be sent. When Status is busy, the value of the Response field is 0 ms. • drop: indicates that the probe packet is discarded because of no link is available. When Status is busy, the value of the Response field is 0 ms.
Address	Destination IP address of an NQA test instance.
Time	Time when the response packet is received.

Related Topics

21.7.4 clear-records

21.7.79 records

21.7.19 display nqa-parameter

Function

The **display nqa-parameter** command displays parameters for the current NQA test instance.

Format

display nqa-parameter

Parameters

None

Views

NQA view

Default Level

1: Monitoring level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display nqa-parameter** command to view parameters available for the current NQA test instance.

Differences between the **display nqa-parameter** and **display this** commands are as follows:

- The **display this** command is used to display commands that have been configured for the test instance. It shows the configuration records.
- The **display nqa-parameter** command is used to display parameters available for the current NQA test instance and prompt which parameter is mandatory for the start of the test instance. Before running the **display nqa-parameter** command, ensure that the type of the test instance is configured.

Example

Display parameters available for the NQA test instance in the NQA view.

```
<Huawei> system-view
[Huawei] nqa test-instance admin icmp
[Huawei-nqa-admin-icmp] test-type icmp
[Huawei-nqa-admin-icmp] description huawei nqa
[Huawei-nqa-admin-icmp] destination-address ipv4 10.1.1.1
[Huawei-nqa-admin-icmp] timeout 5
[Huawei-nqa-admin-icmp] display nqa-parameter
 *: the parameter must be configured before starting the test-instance.
 #: the parameter is undecided.
 <blank>: the parameter is optional.
*test-type                      :icmp
 description                    :huawei nqa
 frequency                      :
 timeout                        :5(default:3)
 threshold rtd                  :
*destination-address type       :ipv4
*destination-address            :10.1.1.1
 source-address type            :
 source-address                 :
 ttl                            :---(default:30)
 datasize                       :
 datafill                       :
 source-interface               :
 sendpacket passroute           :---(default:no)
 probe-count                    :---(default:3)
 send-trap                      :---(default:none)
 test-failtimes                 :---(default:1)
 tos                            :---(default:0)
 fail-percent                   :---(default:100)
 interval                       :---(default:4000)
 vpn-instance                   :
 records history                :---(default:50)
 records result                 :---(default:5)
 records history-filter         :---(default:all)
 agetime                        :---(default:0:0:0)
 ip-forwarding                  :---(default:no)
 nexthop-address type           :
 nexthop-address                :
```


Copyright © Huawei Technologies Co., Ltd.

Table 21-48 Description of the display nqa-parameter command output

Item	Description
test-type	Type of the NQA test instance, which is set using the **test-type** command.
description	Description of the NQA test instance, which is configured using the **description** command.
frequency	Interval at which the NQA test instance is automatically performed, which is set using the **frequency** command.
timeout	timeout period for a probe of an NQA test instance, which is set using the **timeout** command.
threshold rtd	RTD of the NQA test instance, which is set using the **threshold** command.
destination-address type	Destination IP address type of the NQA test instance, which is set using the **destination-address** command.
destination-address	Destination IP address of the NQA test instance, which is set using the **destination-address** command.
source-address type	Source IP address type of the NQA test instance, which is set using the **source-address** command.
source-address	Source IP address of the NQA test instance, which is set using the **source-address** command.
ttl	TTL of the NQA test packet, which is set using the **ttl** command.
datasize	Size of the NQA test packet, which is set using the **datasize** command.
datafill	Pad characters in the NQA test packet, which is set using the **datafill** command.
source-interface	Source interface of the NQA test instance, which is set using the **source-interface** command.
sendpacket passroute	Whether the test instance is configured to send packets without searching the routing table, which is set using the **sendpacket passroute** command.
probe-count	Number of probes for the NQA test instance, which is set using the **probe-count** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
send-trap	Conditions for sending traps for the NQA test instance, which are configured using the **send-trap** command.
test-failtimes	Number of continuous test failures in the NQA test instance, which is set using the **test-failtimes** command.
tos	Type of service (TOS) of the test package in the NQA test instance, which is set using the **tos** command.
fail-percent	Percentage of failed NQA test instances, which is set using the **fail-percent** command.
interval	Interval for sending NQA test packets, which is set using the **interval** command.
vpn-instance	VPN instance name of the NQA test instance, which is set using the **vpn-instance** command.
records history	Maximum number of history records allowed for the NQA test instance, which is set using the **records** command.
records result	Maximum number of test result records allowed for the NQA test instance, which is set using the **records** command.
records history-filter	Filtering records from a historical table for an NQA test instance, referring to the **records history-filter** command.
agetime	Aging time of the NQA test instance, which is set using the **agetime** command.
ip-forwarding	Forwarding IP packets forcibly, which is set using the **ip-forwarding** command.
nexthop-address type	The type of the next hop address, which is set using the **nexthop** command.
nexthop-address	The next hop address, which is set using the **nexthop** command.

Related Topics

21.7.56 nqa

21.7.95 test-type

Copyright © Huawei Technologies Co., Ltd.

21.7.20 display nqa results

Function

The **display nqa results** command displays NQA test results.

Format

display nqa results [**collection** | **success** | **failed**] [**test-instance** *admin-name test-name*] [**verbose**]

Parameters

Parameter	Description	Value
collection	Indicates the total NQA test results.	-
success	Indicates the results of successful tests.	-
failed	Indicates the results of failed tests.	-
test-instance	Indicates an NQA test instance.	-
admin-name	Specifies the name of the administrator for an NQA test instance.	The value must be the name of an existing NQA test instance administrator.
test-name	Specifies the name of an NQA test instance.	The value must be the name of an existing NQA test instance.
verbose	Displays detailed information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

NQA test results cannot be displayed automatically on the terminal. To view NQA test results, run the **display nqa results** command.

If no test instance is specified, the test result of the test instance is displayed in the corresponding test instance view, and the test result of all test instances is displayed in the system view or other views irrelevant to test instances. If a test instance is specified, the test result of only this test instance is displayed.

The **display nqa results** command displays the results of a test instance that has been complete.

Copyright © Huawei Technologies Co., Ltd.

The output of the **display nqa results** command contains the following two parts:

- Universal test results: This part does not vary according to the test instance type.
- Detailed statistics of each test: Statistics items in this part vary according to the test instance type.

The **display nqa results collection** command is used to display the statistics on accumulative results. At present, only the jitter test supports the query of accumulated results.

Precautions

If no optional parameter is specified, all NQA test results are displayed.

When you run the **display nqa results** command to check the results of a single jitter or ICMP jitter test instance:

- If the value of **SendProbe** is 0, no test packet has been sent, and **Packet Loss Ratio** is displayed as 100% (default value).
- If the value of **SendProbe** is not 0 and the value of **Packet Loss Ratio** is 100%, all test packets have been lost.

When you run the **display nqa results collection** command to check the accumulative results of multiple jitter or ICMP jitter test instances:

- If the value of **SendProbe** is 0, no test packet has been sent in these tests, and **Packet Loss Ratio** is displayed as 0% (default value).
- If the value of **SendProbe** is not 0 but the value of **Packet Loss Ratio** is 0%, no test packet has been lost.

Formula used to calculate the accumulative packet loss ratio: Accumulative packet loss ratio = (Accumulative number of sent packets – Accumulative number of received packets)/Accumulative number of sent packets x 100%. If the value of **SendProbe** in the results of a single test is 0, it is not considered during the calculation of the accumulative packet loss ratio.

Example

Display the results of an NQA ICMP test.

```
<Huawei> display nqa results test-instance admin icmp
  NQA entry(admin, icmp) :testflag is inactive ,testtype is icmp
  1 . Test 1 result   The test is finished
   Send operation times: 3              Receive response times: 3
   Completion:success                   RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Status errors number:0
   Destination ip address:10.138.77.21
   Min/Max/Average Completion Time: 2/2/2
   Sum/Square-Sum  Completion Time: 6/12
   Last Good Probe Time: 2012-07-02 17:09:18.1
   Lost packet ratio: 0 %
```

 Copyright © Huawei Technologies Co., Ltd.

Table 21-49 Description of the display nqa results test-instance admin icmp command output

Item	Description
NQA entry(admin, icmp)	NQA test items: • admin: indicates the administrator or creator of the NQA test instance. • icmp: indicates the name of the NQA test instance.
testflag	Test flag. • active: indicates that the test is running. Checking the result of a running test is invalid. • inactive: indicates that the test is complete. At this time, the actual test result is displayed.
testtype	Test type.
1 . Test 1 result	Sequence number of test results. Test results are numbered based on the time when the tests are complete.
The test is finished	Test status: • finished: indicates that the test is complete. • running: indicates that the test is running.
Send operation times	Number of sent packets.
Receive response times	Number of received response packets.
Completion	Completing status of the test: • success: indicates that the test is complete successfully. • no result: indicates that the test is running, and no test result is obtained or no test result is obtained after the test. • failed: indicates that the test fails. • negotiate failed: indicates that the negotiation fails.
RTD OverThresholds number	Number of times that the round-trip delay (RTD) threshold is exceeded.
Attempts number	Test times.
Drop operation number	Number of system resource allocation failures.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Disconnect operation number	Number of forcible disconnections.
Operation timeout number	Number of timeout operations during the test.
System busy operation number	Number of conflict operations.
Connection fail number	Number of times that the local end fails to establish connections with the peer.
Operation sequence errors number	Number of received disordered packets.
RTT Status errors number	Number of RTT status errors.
Destination ip address	Destination IP address of the test.
Min/Max/Average Completion Time	Minimum/Maximum/Average time taken to complete the test.
Sum/Square-Sum Completion Time	Sum and square sum of the time taken to complete the test.
Last Good Probe Time	Time at which the last probe is complete.
Lost packet ratio	Packet loss ratio.

Display the result of an NQA jitter test.

```
<Huawei> display nqa results test-instance admin jitter
 NQA entry(admin, jitter) :testflag is inactive ,testtype is jitter
  1 . Test 1 result   The test is finished
   SendProbe:60                    ResponseProbe:0
   Completion:failed               RTD OverThresholds number:0
   OWD OverThresholds SD number:0      OWD OverThresholds DS number:0
   Min/Max/Avg/Sum RTT:0/0/0/0         RTT Square Sum:0
   NumOfRTT:0                      Drop operation number:0
   Operation sequence errors number:0   RTT Stats errors number:0
   System busy operation number:0      Operation timeout number:60
   Min Positive SD:0               Min Positive DS:0
   Max Positive SD:0               Max Positive DS:0
   Positive SD Number:0              Positive DS Number:0
   Positive SD Sum:0               Positive DS Sum:0
   Positive SD Square Sum:0          Positive DS Square Sum:0
   Min Negative SD:0               Min Negative DS:0
   Max Negative SD:0               Max Negative DS:0
   Negative SD Number:0              Negative DS Number:0
   Negative SD Sum:0               Negative DS Sum:0
   Negative SD Square Sum:0          Negative DS Square Sum:0
   Min Delay SD:0                  Min Delay DS:0
   Avg Delay SD:0                  Avg Delay DS:0
   Max Delay SD:0                  Max Delay DS:0
   Delay SD Square Sum:0             Delay DS Square Sum:0
   Packet Loss SD:0                Packet Loss DS:0
   Packet Loss Unknown:0             Average of Jitter:0
   Average of Jitter SD:0          Average of Jitter DS:0
   Jitter out value:0.0000000        Jitter in value:0.0000000
   NumberOfOWD:0                     Packet Loss Ratio: 100%
   OWD SD Sum:0                    OWD DS Sum:0
   ICPIF value: 0                MOS-CQ value: 0
   TimeStamp unit: ms                Packet Rewrite Number: 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
  Packet Rewrite Ratio: 0%             Packet Disorder Number: 0
  Packet Disorder Ratio: 0%            Fragment-disorder Number: 0
  Fragment-disorder Ratio: 0%          Jitter OverThresholds SD number:0
  Jitter OverThresholds DS number:0    OverallOverThresholds number:0
Start time: 2014-06-25 18:47:05+08:00
End time: 2014-06-25 18:47:05+08:00
```

Table 21-50 Description of the display nqa results test-instance admin jitter command output

Item	Description
NQA entry(admin, jitter)	NQA test items: ● admin: indicates the name of the administrator for an NQA test instance. ● jitter: indicates the name of the NQA test instance.
testflag	Test flag: ● active: indicates that the test is running. Checking the test result during the operation is invalid. ● inactive: indicates that the test is complete. At this time, the actual test result is displayed.
testtype	Test type.
SendProbe	Number of sent probes.
ResponseProbe	Number of received response probes.
Completion	Completing status of the test: ● success: indicates that the test is complete successfully. ● no result: indicates that the test is running, so no result is obtained. ● failed: indicates that the test fails. ● negotiate failed: indicates that negotiation fails. This parameter is displayed only for hardware-based UDP Jitter test instances.
RTD OverThresholds number	Number of times that the RTD threshold is exceeded.
OWD OverThresholds SD number	Number of times that the one-way delay (OWD) threshold (from the source to the destination) is exceeded.
OWD OverThresholds DS number	Number of times that the OWD threshold (from the destination to the source) is exceeded.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Min/Max/Avg/Sum RTT	Minimum/Maximum/Average/Sum of the RTT.
RTT Square Sum	RTT square sum of the probes.
NumOfRTT	Number of RTTs.
Drop operation number	Number of system resource allocation failures.
Operation sequence errors number	Serial number of the error packets received by the client.
RTT Stats errors number	Number of RTT status errors.
System busy operation number	Number of conflict operations.
Operation timeout number	Number of timeout operations during the test.
Min Positive SD	Minimum positive jitter from the source to the destination.
Min Positive DS	Minimum positive jitter from the destination to the source.
Max Positive SD	Maximum positive jitter from the source to the destination.
Max Positive DS	Maximum positive jitter from the destination to the source.
Positive SD Number	Number of the positive jitter from the source to the destination.
Positive DS Number	Number of the positive jitter from the destination to the source.
Positive SD Sum	Sum of the positive jitter from the source to the destination.
Positive DS Sum	Sum of the positive jitter from the destination to the source.
Positive SD Square Sum	Square sum of the positive jitter from the source to the destination.
Positive DS Square Sum	Square sum of the positive jitter from the destination to the source.
Min Negative SD	Minimum negative jitter from the source to the destination.
Min Negative DS	Minimum negative jitter from the destination to the source.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Max Negative SD	Maximum negative jitter from the source to the destination.
Max Negative DS	Maximum negative jitter from the destination to the source.
Negative SD Number	Number of the negative jitter from the source to the destination.
Negative DS Number	Number of the negative jitter from the destination to the source.
Negative SD Sum	Sum of the negative jitter from the source to the destination.
Negative DS Sum	Sum of the negative jitter from the destination to the source.
Negative SD Square Sum	Square sum of the negative jitter from the source to the destination.
Negative DS Square Sum	Square sum of the negative jitter from the destination to the source.
Min Delay SD	Minimum delay from the source to the destination.
Min Delay DS	Minimum delay from the destination to the source.
Avg Delay SD	Average delay from the source to the destination.
Avg Delay DS	Average delay from the destination to the source.
Max Delay SD	Maximum delay from the source to the destination.
Max Delay DS	Maximum delay from the destination to the source.
Delay SD Square Sum	Square sum of the delay jitter from the source to the destination.
Delay DS Square Sum	Square sum of the delay jitter from the destination to the source.
Packet Loss SD	Maximum number of lost packets from the source to the destination.
Packet Loss DS	Maximum number of lost packets from the destination to the source.
Packet Loss Unknown	Number of packets lost at an unknown direction.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Average of Jitter	Average jitter.
Average of Jitter SD	Average jitter from the source to the destination.
Average of Jitter DS	Average jitter from the destination to the source.
Jitter out value	Jitter in sending packets.
Jitter in value	Jitter in receiving packets.
NumberOfOWD	Number of OWD packets.
Packet Loss Ratio	Packet loss ratio.
OWD SD Sum	Sum of OWD from the source to the destination.
OWD DS Sum	Sum of OWD from the destination to the source.
MOS-CQ value	Average estimate of VoIP performance.
ICPIF value	Advantage factor.
TimeStamp unit	Unit of the timestamp.
Packet Rewrite Number	Number of rewritten packets.
Packet Rewrite Ratio	Percentage of rewritten packets to total packets.
Packet Disorder Number	Number of out-of-order packets.
Packet Disorder Ratio	Percentage of out-of-order packets to total packets.
Fragment-disorder Ratio	Percentage of out-of-order fragmented packets to total packets.
Jitter OverThresholds SD number	Number of times that a test instance is successfully performed with the jitter exceeding the specified threshold from the source to the destination.
Jitter OverThresholds DS number	Number of times that a test instance is successfully performed with the jitter exceeding the specified threshold from the destination to the source.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
OverallOverThresholds number	Number of times that a test instance is successfully performed with any of the delays from the source to the destination or from the destination to the source, the bi-directional delay, the jitters from the source to the destination or from the destination to the source exceeding the set threshold.

Display the statistics on the total NQA test results after the packet rewrite check function is configured.

```
<Huawei> display nqa results collection
NQA entry(admin, jitter) :testtype is jitter
  1 . Test 1 collect result
    SendProbe:60                    ResponseProbe:47
    Completion:1                    RTD OverThresholds number:0
    OWD OverThresholds SD number:0      OWD OverThresholds DS number:0
    Min/Max/Avg/Sum RTT:30/1130/296/13910 RTT Square Sum:10840100
    NumOfRTT:47                     Drop operation number:0
    Operation sequence errors number:0   RTT Stats errors number:0
    System busy operation number:0      Operation timeout number:13
    Min Positive SD:10              Min Positive DS:10
    Max Positive SD:260             Max Positive DS:160
    Positive SD Number:9            Positive DS Number:4
    Positive SD Sum:690             Positive DS Sum:230
    Positive SD Square Sum:122900       Positive DS Square Sum:27700
    Min Negative SD:20              Min Negative DS:30
    Max Negative SD:60              Max Negative DS:290
    Negative SD Number:31           Negative DS Number:5
    Negative SD Sum:1010            Negative DS Sum:530
    Negative SD Square Sum:34300        Negative DS Square Sum:105100
    Min Delay SD:15                 Min Delay DS:14
    Avg Delay SD:147                Avg Delay DS:146
    Max Delay SD:565                Max Delay DS:564
    Delay SD Square Sum:2710025         Delay DS Square Sum:2696162
    Packet Loss SD:0                Packet Loss DS:0
    Packet Loss Unknown:0           Average of Jitter:50
    Average of Jitter SD:42         Average of Jitter DS:84
    Jitter out value:0.0000000      Jitter in value:0.0000000
    NumberOfOWD:47                  Packet Loss Ratio: 21%
    OWD SD Sum:6955                 OWD DS Sum:6908
    ICPIF value: 0                  MOS-CQ value: 0
    TimeStamp unit: ms              Packet Rewrite Number: 0
    Packet Rewrite Ratio: 0%        Packet Disorder Number: 0
    Packet Disorder Ratio: 0%       Fragment-disorder Number: 0
    Fragment-disorder Ratio: 0%     Jitter OverThresholds SD number:0
    Jitter OverThresholds DS number:0   OverallOverThresholds number:0
```

Table 21-51 Description of the display nqa results collection command output

Item	Description
SendProbe	Number of sent probes.
ResponseProbe	Number of received response probes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Completion	Number of times that the test is performed.
RTD OverThresholds number	Number of times that the RTD threshold is exceeded.
OWD OverThresholds SD number	Number of times that the OWD threshold (from the source to the destination) is exceeded.
OWD OverThresholds DS number	Number of times that the OWD threshold (from the destination to the source) is exceeded.
Min/Max/Avg/Sum RTT	Minimum/Maximum/Average/Sum of the RTT.
RTT Square Sum	RTT square sum of the probes.
NumOfRTT	Number of RTTs.
Drop operation number	Number of system resource allocation failures.
Operation sequence errors number	Serial number of the error packets received by the client.
RTT Stats errors number	Number of RTT status errors.
System busy operation number	Number of conflict operations.
Operation timeout number	Number of timeout operations during the test.
Min Positive SD	Minimum positive jitter from the source to the destination.
Min Positive DS	Minimum positive jitter from the destination to the source.
Max Positive SD	Maximum positive jitter from the source to the destination.
Max Positive DS	Maximum positive jitter from the destination to the source.
Positive SD Number	Number of the positive jitter from the source to the destination.
Positive DS Number	Number of the positive jitter from the destination to the source.
Positive SD Sum	Sum of the positive jitter from the source to the destination.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Positive DS Sum	Sum of the positive jitter from the destination to the source.
Positive SD Square Sum	Square sum of the positive jitter from the source to the destination.
Positive DS Square Sum	Square sum of the positive jitter from the destination to the source.
Min Negative SD	Minimum negative jitter from the source to the destination.
Min Negative DS	Minimum negative jitter from the destination to the source.
Max Negative SD	Maximum negative jitter from the source to the destination.
Max Negative DS	Maximum negative jitter from the destination to the source.
Negative SD Number	Number of the negative jitter from the source to the destination.
Negative DS Number	Number of the negative jitter from the destination to the source.
Negative SD Sum	Sum of the negative jitter from the source to the destination.
Negative DS Sum	Sum of the negative jitter from the destination to the source.
Negative SD Square Sum	Square sum of the negative jitter from the source to the destination.
Negative DS Square Sum	Square sum of the negative jitter from the destination to the source.
Min Delay SD	Minimum delay from the source to the destination.
Min Delay DS	Minimum delay from the destination to the source.
Avg Delay SD	Average delay from the source to the destination.
Avg Delay DS	Average delay from the destination to the source.
Max Delay SD	Maximum delay from the source to the destination.
Max Delay DS	Maximum delay from the destination to the source.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Delay SD Square Sum	Square sum of the delay jitter from the source to the destination.
Delay DS Square Sum	Square sum of the delay jitter from the destination to the source.
Packet Loss SD	Maximum number of lost packets from the source to the destination.
Packet Loss DS	Maximum number of lost packets from the destination to the source.
Packet Loss Unknown	Number of packets lost at an unknown direction.
Average of Jitter	Average jitter.
Average of Jitter SD	Average jitter from the source to the destination.
Average of Jitter DS	Average jitter from the destination to the source.
Jitter out value	Jitter in sending packets.
Jitter in value	Jitter in receiving packets.
NumberOfOWD	Number of OWD packets.
Packet Loss Ratio	Packet loss ratio.
OWD SD Sum	Sum of OWD from the source to the destination.
OWD DS Sum	Sum of OWD from the destination to the source.
MOS-CQ value	Average estimate of VoIP performance.
ICPIF value	Advantage factor.
TimeStamp unit	Unit of the timestamp.

Related Topics

21.7.4 clear-records

21.7.21 display nqa support-server-type

Function

The **display nqa support-server-type** command displays the server types supported by NQA.

 Copyright © Huawei Technologies Co., Ltd.

Format

display nqa support-server-type

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the server types supported by NQA.

```
<Huawei> display nqa support-server-type
NQA support server type information:

-------------------------------------------------------
  Type            Description
  tcp server      NQA TCP server
  udp server      NQA UDP server
  rtp server      NQA RTP server

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

Table 21-52 Description of the display nqa support-server-type command output

Item	Description
Type	Server types supported by NQA.
Description	Description of the server types supported by NQA

Related Topics

21.7.73 nqa-server tcpconnect

21.7.74 nqa-server udpecho

21.7.22 display nqa support-test-type

Function

The **display nqa support-test-type** command displays the test instance types supported by NQA.

Copyright © Huawei Technologies Co., Ltd.

Format

display nqa support-test-type

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display nqa support-test-type** command to view all test instances supported by the device.

NOTE

You can run this command to view all test instances supported on the device. However, the test instance that can be configured on the device uses the test instanced configured in the **test-type** command as an example.

- If the **display nqa support-test-type** command is run on the NQA server, the test instances supported by the server are displayed.
- If the **display nqa support-test-type** command is run on the NQA client, the test instances supported by the client are displayed.

Example

Display the test instance types supported by NQA.

```
<Huawei> display nqa support-test-type
NQA support test type information:

-------------------------------------------------------
 Type          Description
 tcp           TCP type NQA test
 udp           UDP type NQA test
 http          HTTP type NQA test
 ftp           FTP type NQA test
 jitter        JITTER type NQA test
 icmp          ICMP type NQA test
 snmp          SNMP type NQA test
 trace         TRACE type NQA test
 lspping       LSPPING type NQA test
 lsptrace      LSPTRACE type NQA test
 dns           DNS type NQA test
 dhcp          DHCP type NQA test


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


Copyright © Huawei Technologies Co., Ltd.

Table 21-53 Description of the display nqa support-test-type command output

Item	Description
Type	Test instance types supported by NQA.
Description	Description of the test instance types supported by NQA.

Related Topics

21.7.95 test-type

21.7.23 display nqa-agent

Function

The **display nqa-agent** command displays test status and configuration on an NQA client.

Format

display nqa-agent [*admin-name test-name*] [**verbose**]

Parameters

Parameter	Description	Value
admin-name	Specifies the administrator of an NQA test instance.	The value is a string of 1 to 32 characters.
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 characters.
verbose	Indicates detailed information about the client status of an NQA test.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the client status of an NQA test.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display nqa-agent
  NQA Tests Max:256          NQA Tests  Number:   1
  NQA Flow  Max:256          NQA Flow Remained:256
nqa test-instance admin icmp
 test-type icmp
 destination-address ipv4 192.168.1.2
```

Table 21-54 Description of the display nqa-agent command output

Item	Description
NQA Tests Max	Maximum number of supported NQA test instances.
NQA Tests Number	Number of current NQA test instances.
NQA Flow Max	Maximum number of concurrent NQA test instances.
NQA Flow Remained	Maximum number of concurrent and performable NQA test instances.
test-type	Test type.
destination-address	destination address of a test.

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.92 start

21.7.24 display nqa-ftp-record configuration

Function

The **display nqa-ftp-record configuration** command displays the configuration of NQA test result sent to the FTP server using FTP.

Format

display nqa-ftp-record configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To check the configuration of NQA test result upload to the FTP server through FTP, run the **display nqa-ftp-record configuration** command.

Example

Display the configuration of NQA test result sending to the FTP server using FTP.

```
<Huawei> display nqa-ftp-record configuration
---------------NQA FTP SAVE RECORD CONFIGURATION---------------
  FUNCTION: ENABLE    TRAP: ENABLE
  IP-ADDRESS:10.1.2.8
    SOURCE-ADDRESS:10.1.2.1
  VPN-INSTANCE:
  USERNAME:ftp
  PASSWORD:
  FILENAME:icmp
  ITEM-NUM:100000
  TIME:60
    DATETIMETYPE:UTC
  LAST FINISHED FILENAME:icmp20131214-163628.txt
```

Table 21-55 Description of the display nqa-ftp-record configuration command output

Item	Description
FUNCTION	Whether enable the NQA test results to be sent to the FTP server using FTP. • ENABLE: enabled. • DISABLE: disabled. To set this field, run the **nqa-ftp-record enable** command.
TRAP	Whether send a trap when the NQA test result is saved to the FTP server using FTP. • ENABLE: enabled. • DISABLE: disabled. To set this field, run the **nqa-ftp-record trap-enable** command.
IP-ADDRESS	FTP server address. To set this field, run the **nqa-ftp-record ip-address** command.
SOURCE-ADDRESS	FTP client address. To set this field, run the **nqa-ftp-record source-address** command.
VPN-INSTANCE	VPN instance name.
USERNAME	User name for logging in to the FTP server. To set this field, run the **nqa-ftp-record username** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
PASSWORD	Password for logging in to the FTP server. To set this field, run the **nqa-ftp-record password** command.
FILENAME	Name of a file created at the FTP server. To set this field, run the **nqa-ftp-record filename** command.
ITEM-NUM	Number of NQA test results that are saved to a file using FTP. To set this field, run the **nqa-ftp-record item-num** command.
TIME	Duration of saving NQA test results to a file using FTP. To set this field, run the **nqa-ftp-record time** command.
DATETIMETYPE	Type of time based on which test results are saved to a file on the FTP server: • UTC: worldwide standard time type. • LOCAL: local time type (recommended). To set this field, run the **nqa upload statistics datetime-type** command.
LAST FINISHED FILENAME	Name of a file created at the FTP server last time.

Related Topics

21.7.59 nqa-ftp-record enable
21.7.60 nqa-ftp-record filename
21.7.61 nqa-ftp-record ip-address
21.7.62 nqa-ftp-record item-num
21.7.63 nqa-ftp-record password
21.7.66 nqa-ftp-record source-address
21.7.64 nqa-ftp-record time
21.7.65 nqa-ftp-record trap-enable
21.7.67 nqa-ftp-record username
21.7.75 nqa upload statistics datetime-type

21.7.25 display nqa-server

Function

The **display nqa-server** command displays information about NQA servers.

Copyright © Huawei Technologies Co., Ltd.

Format

display nqa-server

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Both the server and the client need to be configured before starting a TCP, jitter or UDP test instance. Otherwise, the test instances cannot be started.

- In the case of a TCP test instance, the **nqa-server tcpconnect** command needs to be run to enable a TCP server.
- In the case of a jitter or a UDP test instance, the **nqa-server udpecho** command needs to be run to enable a UDP server.

Example

Display the information about NQA servers.

```
<Huawei> display nqa-server

 NQA Server Max: 128              NQA Server Num: 1
 NQA Concurrent TCP Server: 0     NQA Concurrent UDP Server: 1
 NQA Concurrent RTP-UDP Server: 0
nqa-server udpecho 10.1.1.1 6000    ACTIVE    Hardware-based
```

Table 21-56 Description of the display nqa-server command output

Item	Description
NQA Server Max	Maximum number of NQA servers that can be configured.
NQA Server Num	Number of current NQA servers.
NQA Concurrent TCP Server	Number of the configured TCP servers.
NQA Concurrent UDP Server	Number of the configured UDP servers.
NQA Concurrent RTP-UDP Server	Number of the configured RTP-UDP servers.
nqa-server	Running servers.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
ACTIVE	Status of the NQA server.

Related Topics

21.7.73 nqa-server tcpconnect

21.7.74 nqa-server udpecho

21.7.26 display nqa-server session

Function

The **display nqa-server session** command displays the NQA client information on the NQA server.

Format

display nqa-server session

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the **nqa-server session-record enable** command is executed on the NQA server to enable NQA client information display, run the **display nqa-server session** command to view information about all NQA clients connected to the NQA server. The NQA client information includes the IP address of NQA server, IP address of NQA client, source port of NQA client, and VPN.

Precautions

This command is valid for only hardware-based UDP jitter test.

Example

Display NQA client information on the NQA server.

```
<Huawei> display nqa-server session
Total NQA Jitter items = 2
------------------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

```
Server-IP Client-IP Client-Port VPN-INSTANCE
------------------------------------------------------------------
192.168.0.1 192.168.0.255 63081
192.168.0.1 192.168.0.255 53779
------------------------------------------------------------------
```

Table 21-57 Description of the display nqa-server session command output

Item	Description
Total NQA Jitter items	Number of UDP jitter test instances.
Server-IP	IP address of the NQA server.
Client-IP	IP address of the NQA client.
Client-Port	Source port of the NQA client.
VPN-INSTANCE	VPN instance that the server belongs to.

Related Topics

21.7.72 nqa-server session-record enable

21.7.27 display snmp-agent trap feature-name nqa all

Function

The **display snmp-agent trap feature-name nqa all** command displays the status of all traps of the NQA module.

Format

display snmp-agent trap feature-name nqa all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the status of all traps of the NQA module.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display snmp-agent trap feature-name nqa all
------------------------------------------------------------------------------
Feature name: NQA
Trap number : 29
------------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
nqaResultsProbeFailed          on                      on
nqaHTTPStatsProbeFailed        on                      on
pingProbeFailed                on                      on
nqaFTPStatsProbeFailed         on                      on
pingTestFailed                 on                      on
pingTestCompleted              on                      on
traceRouteTestFailed           on                      on
traceRouteTestCompleted        on                      on
nqaResultsTestFailed           on                      on
nqaResultsTestCompleted        on                      on
nqaResultsThresholdNotification
                               on                      on
nqaHTTPStatsTestFailed         on                      on
nqaHTTPStatsTestCompleted      on                      on
nqaHTTPStatsThresholdNotification
                               on                      on
nqaFTPStatsTestFailed          on                      on
nqaFTPStatsTestCompleted       on                      on
nqaFTPStatsThresholdNotification
                               on                      on
nqaJitterStatsTestFailed       on                      on
nqaJitterStatsTestCompleted    on                      on
nqaJitterStatsRTDThresholdNotification
                               on                      on
nqaJitterStatsOWDThresholdNotificationSD
                               on                      on
nqaJitterStatsOWDThresholdNotificationDS
                               on                      on
nqaRisingAlarmNotification     on                      on
nqaFaillingAlarmNotification   on                      on
nqaFtpSaveRecordNotification   on                      on
nqaJitterStatsJitterThresholdNotificationSD
                               on                      on
nqaJitterStatsJitterThresholdNotificationDS
                               on                      on
nqaReflectorStateChangeNotification
                               on                      on
nqaResultsTestResultChange     on                      on
```

Table 21-58 Description of the display snmp-agent trap feature-name nqa all command output

Item	Description
Feature name	Name of the module that a trap belongs to.
Trap number	Number of traps.
Trap name	Name of a trap.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

21.7.28 dns-server

Function

The **dns-server** command configures the IP address of the domain name service (DNS) server in the NQA test.

The **undo dns-server** command deletes the configured IP address of the DNS server.

By default, the IP address of the DNS server is not configured.

Format

dns-server ipv4 *ip-address*

undo dns-server

Parameters

Parameter	Description	Value
ipv4 *ip-address*	Specifies an IPv4 address for the DNS server.	The value is in dotted decimal notation.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before using a DNS test instance to detect the rate of resolving a given DNS name to an IP address, configure a DNS server first.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The test instance can only be a DNS or HTTP test instance.

Precautions

The DNS server configuration of a running test instance cannot be changed.

Example

Set the IP address of the DNS server to 10.1.1.1 in the test named **user test**.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type dns
[Huawei-nqa-user-test] dns-server ipv4 10.1.1.1
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.9 destination-address

21.7.29 fail-percent

Function

The **fail-percent** command sets the failure percentage for the NQA test instance.

The **undo fail-percent** command deletes the configured failure percentage for the NQA test instance.

By default, the failure percentage is 100%. That is, the test is regarded as a failure only when all the probes fail.

Format

fail-percent *percent*

undo fail-percent

Parameters

Parameter	Description	Value
percent	Specifies the percentage of failed probes.	The value is an integer that ranges from 1 to 100.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an NQA test instance, multiple probes are sent to test probe packets. Statistics obtained from multiple probe tests show the network quality.

In actual scenarios, however, a probe test may fail because of interference in the network. In addition, a failure in a probe test does not mean that the NQA test fails. The **fail-percent** command can be used to set failure percentage to check whether an NQA test fails or not. If the number of failure probe packets to the

Copyright © Huawei Technologies Co., Ltd.

total number of probe packets reaches a specified percentage, the NQA test is considered as a failure.

For example, the number of sent packets set in the **probe-count** command is 10, but seven of them are lost during the probe test, the following situations occur:

- If the failure percentage is set to 80, the probe test is considered a success.
- If the failure percentage is set to 60, the probe test is considered a failure.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The failure percentage cannot be set for an FTP, a trace, a LSP Trace, and a DNS test instance.

Precautions

The failure percentage of a running test instance cannot be changed.

Example

Set the percentage of the failed probes to 10% in the test named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] fail-percent 10
```

Related Topics

21.7.76 probe-count

21.7.30 forwarding-simulation inbound-interface

Function

The **forwarding-simulation inbound-interface** command configures a simulated inbound interface.

The **undo forwarding-simulation inbound-interface** command deletes a simulated inbound interface.

By default, no simulated inbound interfaces are configured.

Format

forwarding-simulation inbound-interface *interface-type interface-number*

undo forwarding-simulation inbound-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of a simulated inbound interface.	–

Copyright © Huawei Technologies Co., Ltd.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, NQA test packets are regarded as host packets. The host packets are processed differently with the forwarded packets in that the former is preferably forwarded.

The **forwarding-simulation inbound-interface** command configures a simulated interface through which the NQA test packets, same as the forwarded packets, are forwarded to the product forwarding channel.

In a generalflow test instance, to allow the initiator and reflector to support the lossless mode, run the **forwarding-simulation inbound-interface** *interface-type interface-number* command. This allows the initiator and reflector interfaces to transmit both RFC 2544 and non-RFC 2544 traffic.

Prerequisites

Before configuring a DHCP test instance, configure a DHCP server or DHCP Relay, and ensure reachable routes between the DHCP client and the DHCP server or the DHCP Relay.

Precautions

The type of the test instance must be DHCP test instances.

In the DHCP test instance case, **source-interface** *interface-type interface-number* command and **forwarding-simulation inbound-interface** *interface-type interface-number* command are mutually exclusive. In addition, the DHCP client and NQA DHCP test instance cannot be configured on the same device. Otherwise, the NQA DHCP test instance may fail.

Example

Configure a simulated inbound interface in lossless mode for a DHCP test instance.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type dhcp
[Huawei-nqa-user-test] forwarding-simulation inbound-interface gigabitethernet 1/0/0
```

Related Topics

21.7.90 source-interface

Copyright © Huawei Technologies Co., Ltd.

21.7.31 frequency

Function

The **frequency** command sets the interval at which an NQA test instance is automatically performed.

The **undo frequency** command deletes the configured interval at which an NQA test instance is automatically performed.

By default, the interval at which an NQA test instance is automatically performed is not configured. That is, the test is performed for one time.

Format

frequency *interval*

undo frequency

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an NQA test instance is automatically performed.	The value is an integer that ranges from 1 to 604800, in seconds.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **start** command to set the start time and end time of an NQA test. If you need to perform period test from the start time to the end time in a test instance, run the **frequency** command to set the interval at which an NQA test instance is automatically performed. After that, the NQA test is automatically performed one time at each configured interval.

Configuring the interval of periodic NQA test avoid time-consuming manual operations.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Precautions

The **frequency** value must comply with the following rules:

Copyright © Huawei Technologies Co., Ltd.

- In the DHCP, DNS, FTP, HTTP, or Trace test instance, the **frequency** value must be larger than the product of **timeout** and **probe-count**.
- In the ICMP, SNMP, TCP, or UDP test instance, the **frequency** value must be larger than the product of **interval**and **probe-count**.
- In the Jitter test instance:

  frequency > **probe-count** × **jitter-packetnum** × **interval** + **timeout**
- In the hardware-based Jitter test instance:

  frequency > **probe-count** × **jitter-packetnum** × **interval** + 6200 + (5 × **timeout**/3)

  The unit of 6200 is ms.
- may be returned if the following condition is true: Interval at which the NQA test is automatically performed ≤ (Number of sent packets -1) x Interval + Timeout period + 1. For a test instance with jitter-packetnum configured, the number of sent packets is Probe-count x jitter-packetnum.

For trace and LSP trace test instances, the interval must be larger than or equal to 60 seconds.

If no end time is configured, the test cannot stop automatically. You need to stop it manually. The frequency of a running test instance cannot be changed.

Example

Set the interval at which test instance **user test** is automatically performed to 20 seconds.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] frequency 20
```

21.7.32 ftp-filename

Function

The **ftp-filename** command configures the file name and file path for an NQA FTP test instance.

The **undo ftp-filename** command deletes the file name and file path for an NQA FTP test instance.

By default, no file name and file path are configured.

Format

ftp-filename *file-name*

undo ftp-filename

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
file-name	Specifies the name and path of the operation file in an FTP test instance.	The value is a string of 1 to 230 characters.

Views

NQA view

Default Level

3: Management level

Usage Guidelines

The **ftp-filename** command is valid only for FTP test instances.

You cannot change the file path and file name of a running test instance.

If no file path is specified, the system searches for the file in the current path.

The file name cannot end with any forward slashes (/) or backward slashes (\).

The file name includes but is not limited to the extension name, such as .txt.

NOTE

Various FTP servers may support files with the file name in different length ranges. Before you configure this command, ensure that the target FTP server supports the length of the specified file name. Otherwise, NQA test results may fail to be transmitted using FTP.

Example

Set the FTP path and file name of test instance **user test** to **D:\abc** and **abc.txt** respectively.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type ftp
[Huawei-nqa-user-test] ftp-filename D:\abc\abc.txt
```

Related Topics

21.7.56 nqa

21.7.34 ftp-operation

21.7.95 test-type

21.7.33 ftp-filesize

Function

The **ftp-filesize** command sets the size of the file used in an NQA FTP test instance.

Copyright © Huawei Technologies Co., Ltd.

The **undo ftp-filesize** command restores the default size of the file used in an NQA FTP test instance.

By default, the size of the file used in the FTP test is 1000 Kbytes.

Format

ftp-filesize *size*

undo ftp-filesize

Parameters

Parameter	Description	Value
size	Specifies the size of the file used in the FTP test.	The value is an integer that ranges from 1 to 10000, in Kbytes.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

You cannot change the configured size of the file when the test is running.

If specifying the size of the upload file is adopted, the FTP client automatically generates the file name **nqa-ftp-test.txt**. If the test is performed several times, the newly uploaded file replaces the previous one.

The type of the test instance has been set to **ftp** using the **test-type** command.

Example

Set the size of the file to 1024 bytes in the FTP upload test named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type ftp
[Huawei-nqa-user-test] ftp-filesize 1024
```

Related Topics

21.7.34 ftp-operation

21.7.95 test-type

Copyright © Huawei Technologies Co., Ltd.

21.7.34 ftp-operation

Function

The **ftp-operation** command sets the operation mode for an NQA FTP test instance.

The **undo ftp-operation** command restores the default operation mode of an NQA FTP test instance.

By default, the operation mode of an FTP test instance is **get**.

Format

ftp-operation { **get** | **put** }

undo ftp-operation put

Parameters

Parameter	Description	Value
get	Indicates that the client downloads a file from the server and the download speed is recorded.	-
put	Indicates that the client uploads a local file or a created file to the server and the upload speed is recorded.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the FTP download test, the local device functions as an FTP client to download/upload the specified file from/to the FTP server. Statistics about each FTP phase are displayed, including the time to set up an FTP control connection and the time to transmit data.

The **ftp-operation** command can be used to specify the FTP operation mode as **put** or **get**. A connection with the FTP server is set up using the IP address, the user name, and the password of the FTP server, and the time to set up FTP connection is recorded.

Prerequisites

The type of the test instance has been set to **ftp** using the **test-type** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The operation mode of a running test instance cannot be changed.

Example

Perform a test named **user test** to obtain the FTP download speed.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type ftp
[Huawei-nqa-user-test] ftp-operation get
```

Related Topics

21.7.33 ftp-filesize

21.7.32 ftp-filename

21.7.95 test-type

21.7.35 ftp-password

Function

The **ftp-password** command sets a password for logging in to the FTP server in an NQA FTP test instance.

The **undo ftp-password** command deletes the configured password for logging in to the FTP server.

By default, no password is set for FTP test instances.

Format

ftp-password { *password* | **cipher** *cipher-password* }

undo ftp-password

Parameters

Parameter	Description	Value
password	Specifies the password for logging in to the FTP server in an FTP test instance.	The value is a string of 1 to 32 or 32 to 68 case-sensitive characters without spaces. • The length of a plaintext password ranges from 1 to 32. • The length of a ciphertext password ranges from 32 to 68. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher *cipher-password*	Specifies the password for logging in to the FTP server in an FTP test instance.	The value is a string of 1 to 32 or 32 to 68case-sensitive characters without spaces. • The length of a plaintext password ranges from 1 to 32. • The length of a ciphertext password ranges from 32 to 68. • If the password length is 32 and the configured ciphertext password can be decrypted successfully, the configured ciphertext password takes effect. If the configured ciphertext password cannot be decrypted, the plaintext password is used after passing the validity check. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the FTP test, the local device functions as an FTP client to download/upload the specified file from/to the FTP server. Statistics about each FTP phase are displayed, including the time to set up an FTP control connection and the time to transmit data.

To ensure test security and prevent unauthorized users from accessing the network, you need to enable identity authentication. The **ftp-password** command

 Copyright © Huawei Technologies Co., Ltd.

can be used to set the specified user and password. Only the user who enters the authorized user name and password is authorized to access the network.

Prerequisites

The type of the test instance has been set to **ftp** using the **test-type** command.

Precautions

The password of a running test instance cannot be changed.

Example

Set the password for logging in to the FTP server to **Huawei-123**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type ftp
[Huawei-nqa-user-test] ftp-password Huawei-123
```

Related Topics

21.7.36 ftp-username

21.7.95 test-type

21.7.36 ftp-username

Function

The **ftp-username** command sets the user name for logging in to the FTP server in an FTP test instance.

The **undo ftp-username** command deletes the configured user name for logging in to the FTP server.

By default, no user name is set for FTP test instances.

Format

ftp-username *name*

undo ftp-username

Parameters

Parameter	Description	Value
name	Specifies the user name for logging in to the FTP server.	The value is a string of 1 to 255 case-sensitive characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

NQA view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the FTP test, the local device functions as an FTP client to download/upload the specified file from/to the FTP server. Statistics about each FTP phase are displayed, including the time to set up an FTP control connection and the time to transmit data.

To ensure test security and prevent unauthorized users from accessing the network, you need to enable identity authentication. The **ftp-username** command can be used to set the specified user in an FTP test. Only the user who enters the authorized user name and password is authorized to access the network.

Prerequisites

The type of the test instance has been set to **ftp** using the **test-type** command.

Precautions

The user name of a running test instance cannot be changed.

Example

Set the user name for logging in to the FTP server to **user1**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type ftp
[Huawei-nqa-user-test] ftp-username user1
```

Related Topics

21.7.35 ftp-password
21.7.95 test-type

21.7.37 hardware-based enable

Function

The **hardware-based enable** command enables the hardware forwarding engine on the LPU to send packets and add timestamps to the packets during the jitter test.

The **undo hardware-based** command disables the hardware forwarding engine on the LPU from sending packets and adding timestamps to the packets during the jitter test.

By default, the hardware forwarding engine on the LPU is not enabled to send packets and add timestamps to the packets.

Format

hardware-based enable

Copyright © Huawei Technologies Co., Ltd.

undo hardware-based

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **hardware-based enable** command can only be used in the jitter test to enable the hardware forwarding engine on the LPU to send packets and add timestamps to the packets.

After the **hardware-based enable** command is configured, the **sendpacket passroute** can be configured, but does not take effect.

Example

Enable the hardware forwarding engine on the LPU to send packets and add timestamps to the packets.

```
<Huawei> system-view
[Huawei] nqa test-instance admin jitter
[Huawei-nqa-admin-jitter] test-type jitter
[Huawei-nqa-admin-jitter] hardware-based enable
```

Related Topics

21.7.95 test-type

21.7.38 http-operation

Function

The **http-operation** command sets the operation mode for an NQA HTTP test instance.

By default, the operation mode of the HTTP test instance is GET.

Format

http-operation get

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
get	Obtains data from the HTTP server.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

This command applies only to the HTTP test.

You cannot change the operation mode of a running HTTP test instance.

Example

Set the operation mode of HTTP test instance **user test** to **get**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type http
[Huawei-nqa-user-test] http-operation get
```

Related Topics

21.7.39 http-url

21.7.95 test-type

21.7.39 http-url

Function

The **http-url** command configures the uniform resource locator (URL) and version information for an HTTP test instance.

The **undo http-url** command deletes the configured URL and version information.

By default, no URL or version information is configured for an HTTP test instance.

Format

http-url *deststring* [*verstring*]

undo http-url

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
deststring	Specifies the name of the web page used for an HTTP test.	The value is a string of 1 to 230 case-insensitive characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.
verstring	Specifies the HTTP version.	It can be set to v1.0 or 1.1. The default HTTP version is v1.0.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

HTTP1.0 and HTTP1.1 are supported in this test instance.

Precautions

The **http-url** command applies only to HTTP test instances. You cannot change the URL of a running HTTP test instance.

The URL of a HTTP test instance must be a URL that is displayed in a browser.

Example

Set the URL of HTTP test instance **user test** to **http://www.example.com**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type http
[Huawei-nqa-user-test] http-url http://www.example.com
```

Related Topics

21.7.38 http-operation

21.7.95 test-type

21.7.40 icmp-jitter-mode

Function

The **icmp-jitter-mode** command sets the type of ICMP jitter test instance.

The **undo icmp-jitter-mode** command restores the default type of ICMP jitter test instance.

Copyright © Huawei Technologies Co., Ltd.

By default, the ICMP jitter test type is icmp-timestamp.

Format

icmp-jitter-mode { **icmp-echo** | **icmp-timestamp** }

undo icmp-jitter-mode

Parameters

Parameter	Description	Value
icmp-echo	Configures the ICMP jitter test instance to use ICMP echo packets.	-
icmp-timestamp	Configures the ICMP jitter test instance to use ICMP timestamp packets.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

In an ICMP jitter test, icmp-timestamp has a higher calculation precision of jitter parameters (such as delay and jitter) than icmp-echo. Therefore, icmp-timestamp is recommended.

NOTE

If the remote device does not support icmp-timestamp or requires ICMP echo packets, configure icmp-echo.

Example

Configure the ICMP jitter test instance to use ICMP echo packets.

```
<Huawei> system-view
[Huawei] nqa test-instance admin icmpjitter
[Huawei-nqa-admin-icmpjitter] test-type icmpjitter
[Huawei-nqa-admin-icmpjitter] icmp-jitter-mode icmp-echo
```

Related Topics

21.7.95 test-type

21.7.41 interval (NQA view)

Function

The **interval** command sets the interval at which NQA test packets are sent.

Copyright © Huawei Technologies Co., Ltd.

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

- The interval is 20 milliseconds for a jitter test instance.
- The interval is 4 seconds for other test instances.

Format

interval { **milliseconds** *interval* | **seconds** *interval* }

undo interval

Parameters

Parameter	Description	Value
milliseconds *interval*	Sets the interval at which packets are sent, in milliseconds. **NOTE** If the configured interval is a multiple of 1000 milliseconds, the system will automatically convert milliseconds into seconds.	The value is an integer that ranges from 10 to 60000.
seconds *interval*	Sets the interval at which packets are sent, in seconds.	The value is an integer that ranges from 1 to 60, in seconds.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an NQA test instance, multiple probes are sent. Statistics obtained from multiple probe tests show the network quality. Probe packets (or probes) are sent at a specified interval.

- If the network quality is poor, the interval at which packets are sent must be increased. Otherwise, the network performance may deteriorate.
- If the network quality is good, the interval at which are sent can be decreased to shorten the waiting time.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The type of a test instance has been specified using the **test-type** command. The **interval** command is valid only for the jitter, ICMP, SNMP, LSP Ping, TCP, and UDP test instances.

Configuration Impact

- If the configured interval is a multiple of 1000 milliseconds, the system will automatically convert milliseconds into seconds.
- Packets can be sent at interval of milliseconds only in jitter test instances. The interval at which packets are sent must be greater than the timeout period set using the **timeout** command in all test instances except the jitter test instance.
- If the interval for sending packets has been configured, running the **interval** command will override the previous configuration.

Precautions

- The interval for sending packets of a running test instance cannot be changed.
- The interval for sending UDP jitter test packets must be less than 1 second.

Example

Set the interval for sending test packets to 1000 milliseconds.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] interval milliseconds 1000
```

21.7.42 ip nqa-compatible responder enable

Function

The **ip nqa-compatible responder enable** command enables the device to respond to UDP-Echo or UDP-Jitter packets sent by a third-party device or NMS software.

The **undo ip nqa-compatible responder enable** command disables the device from responding to UDP-Echo or UDP-Jitter packets sent by a third-party device or NMS software.

By default, the device is disabled from responding to UDP-Echo or UDP-Jitter packets sent by a third-party device or NMS software.

Format

ip nqa-compatible responder [**vpn-instance** *vpn-instance-name*] **enable**

undo ip nqa-compatible responder [**vpn-instance** *vpn-instance-name*] **enable**

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the VPN instance of the third-party device or NMS software.	The VPN instance has been created on the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device connects a third-party device or NMS software, run the **ip nqa-compatible responder enable** command to enable the device to respond to UDP-Echo or UDP-Jitter packets sent by the third-party device or NMS software.

Example

Enable the device to respond to UDP-Echo or UDP-Jitter packets sent by a third-party device or NMS software.

```
<Huawei> system-view
[Huawei] ip nqa-compatible responder enable
```

Related Topics

21.7.44 ip nqa-compatible udp

21.7.43 ip nqa-compatible auto

21.7.43 ip nqa-compatible auto

Function

The **ip nqa-compatible auto** command configures the device to respond to UDP-Echo or UDP-Jitter packets sent from a third-party device or NMS software.

The **undo ip nqa-compatible auto** command configures the device not to respond to UDP-Echo or UDP-Jitter packets sent from a third-party device or NMS software.

By default, the device does not respond to UDP-Echo or UDP-Jitter packets sent from a third-party device or NMS software.

Format

ip nqa-compatible auto

undo ip nqa-compatible auto

Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device works with a third-party device or software to perform UDP-Echo or UDP-Jitter tests, this command allows the device to respond to UDP-Echo or UDP-Jitter packets sent from the third-party device or NMS software.

Prerequisites

The **ip nqa-compatible responder enable** command has been executed in the device view to enable the capability to respond to the UDP-Echo or UDP-Jitter packets sent from the a third-party device or NMS software.

Precautions

If the **ip nqa-compatible udp** command has been configured, the **ip nqa-compatible auto** command does not take effect. Run the **undo ip nqa-compatible udp** first.

Example

Configure the device to respond to UDP-Echo or UDP-Jitter packets sent from a third-party device or NMS software.

```
<Huawei> system-view
[Huawei] ip nqa-compatible auto
```

Related Topics

21.7.44 ip nqa-compatible udp

21.7.42 ip nqa-compatible responder enable

21.7.44 ip nqa-compatible udp

Function

The **ip nqa-compatible udp** command configures the IP address, port number, and service type of the response to the UDP-Echo or UDP-Jitter packets sent by a third-party device or NMS software.

The **undo ip nqa-compatible udp** command deletes the IP address, port number, and service type of the response to the UDP-Echo or UDP-Jitter packets sent by a third-party device or NMS software.

Copyright © Huawei Technologies Co., Ltd.

By default, the IP address, port number, and service type of the response to the UDP-Echo or UDP-Jitter packets sent by a third-party device or NMS software are not configured.

Format

ip nqa-compatible { **device** | **network-management** } **udp** *ip-address* [**vpn-instance** *vpn-instance-name*] *port-number* [*tos-value*]

undo ip nqa-compatible { **device** | **network-management** } **udp** *ip-address* [**vpn-instance** *vpn-instance-name*] *port-number* [*tos-value*]

Parameters

Parameter	Description	Value
device	Specifies a third-party device.	-
network-management	Specifies a third-party NMS software.	-
ip-address	Specifies the IP address of the third-party device or NMS software.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the VPN instance of the third-party device or NMS software.	The VPN instance has been created on the device.
port-number	Specifies the port number of the third-party device or NMS software.	The value is an integer that ranges from 0 to 65535.
tos-value	Specifies the service type of the third-party device or NMS software.	The value is an integer that ranges from 0 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device connects to the third-party device or NMS software and needs to respond to the UDP-Echo or UDP-Jitter packets sent by the third-party device or NMS software, run this command to specify the IP address, port number, and service type of the response. This command helps improving the accuracy and security of NQA tests.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The **ip nqa-compatible responder** [**vpn-instance** *vpn-instance-name*] **enable** command has been executed in the system view to enable the device to respond to the UDP-Echo or UDP-Jitter packets sent by the third-party device or NMS software.

Precaution

If the configured port number is 7, 13, or 19, run the **undo anti-attack udp-flood enable** command to disable UDP Flood attack defense before running the **ip nqa-compatible udp** command. Otherwise, the device discards UDP-Echo or UDP-Jitter packets. If the configured port number is occupied by another process, the **ip nqa-compatible udp** command fails to take effect.

If the **ip nqa-compatible auto** command has been configured, the **ip nqa-compatible udp** command does not take effect. Run the **undo ip nqa-compatible auto** first.

Example

Set the IP address to 10.1.1.1, port number to 2000, and service type to 10 for the response to the UDP-Echo or UDP-Jitter packets sent by the third-party.

```
<Huawei> system-view
[Huawei] ip nqa-compatible device udp 10.1.1.1 2000 10
```

Related Topics

21.7.43 ip nqa-compatible auto

21.7.42 ip nqa-compatible responder enable

21.7.45 ip-forwarding

Function

The **ip-forwarding** command configures packets to be forcibly forwarded using IP on the first node.

The **undo ip-forwarding** command disables packets from being forcibly forwarded using IP on the first node.

Format

ip-forwarding

undo ip-forwarding

Parameters

None

Views

NQA view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

When a fault occurs on the network, you can first run the **ping** command to check network connectivity. On an MPLS network, if a fault occurs but the control layer fails to detect the fault, the ping operation fails. To fast identify whether the fault occurs on the MPLS network or on the IP network, you can configure IP packets to be forcibly forwarded using IP on the first node. This can help you fast locate the fault.

NOTE

Currently, only NQA ICMP test instances support this configuration.

Example

Configure packets to be forwarded using IP.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] ip-forwarding
```

Related Topics

21.7.95 test-type

21.7.46 jitter-codec

Function

The **jitter-codec** command configures a code type for an NQA jitter simulated voice test.

The **undo jitter-codec** command deletes the configured code type of an NQA jitter simulated voice test.

By default, an NQA jitter test is not a simulated voice test.

Format

jitter-codec { **g711a** | **g711u** | **g729a** }

undo jitter-codec

Parameters

Parameter	Description	Value
g711a	Sets the code type of a simulated voice test to g711alaw. The transmission rate of g711alaw is 64 kbit/s.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
g711u	Sets the code type of a simulated voice test to g711ulaw. The transmission rate of g711ulaw is 64 kbit/s.	-
g729a	Sets the code type of a simulated voice test to g729a. The transmission rate of g729a is 8 kbit/s.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **jitter-codec** command can be used to configure the code types of conversion between simulated voice signals and digital signals to detect VoIP services in jitter test instances. You can specify different code types for VoIP services in actual situations.

The size of a jitter test packet varies with the code type.

- If the code type is **g711a**, the packet size configured using the **datasize** *size* command is 172 bytes.
- If the code type is **g711u**, the packet size configured using the **datasize** *size* command is 172 bytes.
- If the code type is **g729a**, the packet size configured using the **datasize** *size* command is 32 bytes.

The differences between g711a, g711u, and g729a of a jitter test instance are as follows:

Table 21-59 Differences between the code types

Code Type	Length of Data Area	Number of the Sent Packets	Interval at Which Packets Are Sent
g711a	172 bytes	1000	20 ms
g711u	172 bytes	1000	20 ms
g729a	32 bytes	1000	20 ms

After configuring the code type, run the **adv-factor** command to configure an advantage factor to simulate the jitter of actual voice packets.

After configuring the **jitter-codec** and **adv-factor** commands in a jitter test instance, you can adjust test packets to simulate the sending of VoIP traffic. This simulation helps to detect VoIP network and analyze service traffic.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- The actual code types of the VoIP services to be tested have been set to the same.
- The test instance type has been set to jitter using the **test-type jitter** command.
- The remote device has been enabled to respond to the jitter test using the **nqa-server udpecho** command.

Configuration Impact

- If a code type has been configured, running the **jitter-codec** command will override the previous configuration.
- If a code type is changed, the configured advantage factor does not take effect and you need to configure a new advantage factor.

Precautions

The code type of a running test instance cannot be changed.

Example

Set the code type of a simulated voice test case to g711a.

```
<Huawei> system-view
[Huawei] nqa test-instance admin jitter
[Huawei-nqa-admin-jitter] test-type jitter
[Huawei-nqa-admin-jitter] jitter-codec g711a
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.1 adv-factor

21.7.47 jitter-packetnum

Function

The **jitter-packetnum** command sets the number of packets sent in each probe test instance.

The **undo jitter-packetnum** command restores the default number of packets sent in each probe test instance.

By default, 20 test packets are sent in each probe.

Format

jitter-packetnum *number*

undo jitter-packetnum

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Specifies the number of test packets sent in each probe in the jitter test (**probe-count**).	The value is an integer that ranges from 1 to 3000. The default value is 20.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an NQA test instance, the **jitter-packetnum** command can be used to set the number of consecutive packets to simulate the actual traffic of a data in a specified period of time. This helps simulate services more accurately.

For example, the **jitter-packetnum** command can be used to set the number of consecutive packets to 3000 and an interval of 20 ms to send packets. In this way, G.711 traffic can be simulated within one minute to detect VoIP services in UDP jitter test instances.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The number of sent packets can be configured only for jitter test instances.

Configuration Impact

- In jitter test instances, the number of sent packets = **jitter-packetnum** x **probe-count**, but the product cannot exceed 3000.
- If the number of probe packets has been set, running the **jitter-packetnum** command will override the previous configuration.

Precautions

The number of probe packets of a running test instance cannot be changed.

Example

Perform 3 probes in the test named **user test** and send 1000 packets in each probe.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] probe-count 3
[Huawei-nqa-user-test] jitter-packetnum 1000
```


Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.41 interval (NQA view)
21.7.76 probe-count

21.7.48 lsp-exp

Function

The **lsp-exp** command configures the LSP EXP value of MPLS Echo Request packets in an NQA test instance.

Using the **undo lsp-exp** command, you can restore the default setting.

By default, LSP EXP is 0.

Format

lsp-exp *exp*

undo lsp-exp

Parameters

Parameter	Description	Value
exp	Specifies the LSP EXP value of an NQA test instance.	The value is an integer that ranges from 0 to 7. The default value is 0.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NOTE

The AR100&AR120&AR150&160&200 does not support the **lsp-exp** command.

The MPLS experimental bits (EXP) field is a 3-bit field in the MPLS header used to mark the precedence of MPLS packets.

Test packets are added to different queues according to their LSP EXP values, so that

- Congestion on the link can be avoided.
- Specified queue can be detected.

Precautions

Copyright © Huawei Technologies Co., Ltd.

This command applies to only the LSP test.

You cannot change the configured LSP EXP value when the test is performed.

Example

Set the LSP EXP value to 5.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type lspping
[Huawei-nqa-user-test] lsp-exp 5
```

Related Topics

21.7.95 test-type

21.7.49 lsp-path full-display

Function

Using the **lsp-path full-display** command, you can view all devices, including Ps, along an LSP in the NQA test result.

Using the **undo lsp-path full-display** command, you can view all devices, except for Ps, along an LSP in the NQA test result.

By default, you can view only PEs, not Ps, along an LSP in the NQA test result.

Format

lsp-path full-display

undo lsp-path full-display

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **lsp-path full-display** command can be used to display all devices, including Ps, along an LSP in the NQA test result. At present, this command is available only for VPLS PW trace test instances.

After the **lsp-path full-display** command is run, you can view all devices, including Ps, along an LSP in the result of a VPLS PW trace test instance. Otherwise, you can view only PEs along an LSP.

Copyright © Huawei Technologies Co., Ltd.

Example

Display all devices, including Ps, along an LSP in the result of a VPLS PW trace test instance.

```
<Huawei> system-view
[Huawei] nqa test-instance vplspw trace
[Huawei-nqa-vplspw-trace] test-type vplspwtrace
[Huawei-nqa-vplspw-trace] lsp-path full-display
```

Related Topics

21.7.95 test-type

21.7.50 lsp-nexthop

Function

The **lsp-nexthop** command is used to configure the IP address of the next hop in the case that load balancing is enabled.

Using the **undo lsp-nexthop** command, you can cancel the current setting.

By default, the next-hop IP address of any link that participates in load balancing.

Format

lsp-nexthop *nexthop-ip-address*

undo lsp-nexthop

Parameters

Parameter	Description	Value
nexthop-ip-address	Specifies the next hop address.	It is in dotted decimal notation.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NOTE

The AR100&AR120&AR150&160&200 does not support the **lsp-nexthop** command.

Two conditions must be meet before you use the command:

Copyright © Huawei Technologies Co., Ltd.

- **lsp-type** is IPv4
- **lsp-version** is RFC4379

You can use the **lsp-nexthop** command to configure the IP address of the next hop. Test instance type supported as following:

- LSP Ping
- LSP Trace

Precautions

A running test instance cannot be configured with the next hop address.

Example

Specify the next hop address for the LSP Ping test instance whose LSP type is IPv4 and lsp-version is rfc4379.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type lspping
[Huawei-nqa-user-test] lsp-type ipv4
[Huawei-nqa-user-test] lsp-version rfc4379
[Huawei-nqa-user-test] lsp-nexthop 10.1.2.20
```

Related Topics

21.7.95 test-type

21.7.53 lsp-type

21.7.51 lsp-replymode

Function

Using the **lsp-replymode** command, you can set the reply mode for the LSP test.

Using the **undo lsp-replymode** command, you can restore the default setting.

By default, UDP packets are used.

Format

lsp-replymode { **no-reply** | **udp** | **udp-via-vpls** | **udp-router-alert** | **level-control-channel** }

undo lsp-replymode

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
no-reply	Indicates that the LSP test is not responded.	If the **no-reply** parameter is specified in the command, the destination does not respond to NQA probe packets. This configuration is used to collect the statistics on or process received probe packets on the destination host, and no response packets need to be sent. The NQA test instance fails because the client does not receive response packets.
udp	Indicates that IPv4 UDP packets are used to respond to the LSP test.	-
udp-via-vpls	Indicates that VPLS UDP packets are used to respond to the LSP test.	-
udp-router-alert	Indicates that VPLS UDP packets are used to respond to the LSP test.	-
level-control-channel	Indicates that the reply packets are sent through the application-level control channel.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NOTE

The AR100&AR120&AR150&160&200 does not support the **lsp-replymode** command.

Using the **lsp-replymode** command, you can set the reply mode for the LSP test. The following test instances are supported:

- LSP Ping
- LSP Trace

 Copyright © Huawei Technologies Co., Ltd.

Precautions

lsp-replymode no-reply indicates the unidirectional test. If the client displays timeout, it indicates that the test succeeds.

You cannot change the reply mode of the currently performed LSP test.

Example

Set the reply mode of the test named **user test** to sending UDP packets.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type lspping
[Huawei-nqa-user-test] lsp-replymode udp
```

Related Topics

21.7.95 test-type

21.7.52 lsp-tetunnel

Function

The **lsp-tetunnel** command configures the TE tunnel used in an NQA LSP test.

The **undo lsp-tetunnel** command deletes the configured TE tunnel.

By default, no TE tunnel is configured for an LSP test instance.

Format

lsp-tetunnel tunnel *interface-number* [**hot-standby** | **primary**]

undo lsp-tetunnel

Parameters

Parameter	Description	Value
tunnel *interface-number*	Specifies the tunnel interface number.	-
hot-standby	Indicates the hot-standby tunnel of the TE tunnel.	-
primary	Indicates the primary tunnel of the TE tunnel.	-

Views

NQA view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Prerequisites

NOTE

The AR100&AR120&AR150&160&200 does not support the **lsp-tetunnel** command.

Before using the **lsp-tetunnel** command to configure the TE tunnel in an NQA LSP test instance, run the **lsp-type te** command to specify the NQA LSP test type to TE.

You cannot change the TE tunnel when the LSP test is performed.

Example

Configure the TE tunnel of the test named **user test**.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] quit
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type lspping
[Huawei-nqa-user-test] lsp-type te
[Huawei-nqa-user-test] lsp-tetunnel tunnel 0/0/1
```

Configure the CR-LSP hot-standby tunnel of the test named **user test**.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] quit
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type lspping
[Huawei-nqa-user-test] lsp-type te
[Huawei-nqa-user-test] lsp-tetunnel tunnel 0/0/1 hot-standby
```

Related Topics

21.7.95 test-type

21.7.53 lsp-type

21.7.53 lsp-type

Function

Using the **lsp-type** command, you can configure the LSP test type.

Using the **undo lsp-type** command, you can cancel configuring the LSP test type.

By the default, the value of lsp-type is ipv4.

Format

lsp-type { **ipv4** | **te** | **ipv4-vpn** }

undo lsp-type

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv4	Sets the test type to Ipv4 LSP ping/trace.	-
te	Sets the type to LSP ping/trace of the TE tunnel.	-
ipv4-vpn	Sets the LSP test type to IPv4 L3VPN.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NOTE

The AR100&AR120&AR150&160&200 does not support the **lsp-type** command.

The **lsp-type** command can be used to configure the LSP test type of an NQA test instance to detect an LDP or a TE tunnel.

- If **ipv4** is configured, the NQA test instance is used to detect the connectivity of a specified LDP LSP. The destination address of the test instance is configured using the **destination-address** command.
- If **te** is configured, the NQA test instance is used to detect the connectivity of a specified TE tunnel. The destination address of the test instance is configured using the **lsp-tetunnel** command.
- If the **ipv4-vpn** parameter is set, the NQA test case is used to test LSPs on a BGP-based L3VPN network.
  - To test a primary LSP on a BGP-based L3VPN network, specify the destination address using the **destination-address lsp-masklen** *masklen* command.
  - To test a primary LSP on a BGP-based L3VPN network, specify the destination address using the **destination-address lsp-masklen** *masklen* **vpn-frr-path** command.

Prerequisites

- If the LSP test type is set to IPv4, the NQA test instance type must be set to LSP ping or LSP trace.
- If the LSP test type is set to TE, the NQA test instance type must be set to LSP ping or LSP trace.
- If the LSP test type is set to IPv4 L3VPN, the NQA test instance type must be set to LSP ping.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The type of an LSP test that is running cannot be changed.

Example

Set the type of the test named **user test** to Ipv4 LSP ping.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type lspping
[Huawei-nqa-user-test] lsp-type ipv4
```

Related Topics

21.7.95 test-type

21.7.54 lsp-version

Function

Using the **lsp-version** command, you can configure the protocol that is used by the LSP test instance.

Using the **undo lsp-version** command, you can restore the default setting.

By default, draft6 is adopted.

Format

lsp-version { **rfc4379** | **draft6** | **ptn-mode** }

undo lsp-version

Parameters

Parameter	Description	Value
rfc4379	Indicates that the protocol defined in RFC 4379 is adopted.	-
draft6	Indicates that Draft-ietf-mpls-lsp-ping-06 is adopted.	-
ptn-mode	Indicates that trace VC packets are replied in a multi-segment PW scenario.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The AR100&AR120&AR150&AR160&200 does not support the **lsp-version** command.

The **lsp-version** command can be used to specify the protocol that is used by the LSP test instance.

Prerequisites

If **draft6** or **rfc4379** is specified in the **lsp-version** command, specify **lspping** or **lsptrace** in the **test-type** command.

NOTE

The protocol adopted by a running LSP test instance cannot be changed.

Example

Configure the LSP test instance to use the protocol defined in RFC 4379.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type lspping
[Huawei-nqa-user-test] lsp-version rfc4379
```

Related Topics

21.7.95 test-type

21.7.55 nexthop

Function

The **nexthop** configures a next hop address for NQA test packets.

The **undo nexthop** deletes the configured next hop address for the NQA test packets.

By default, the next hop address for the NQA test packets is obtained by searching the routing table.

Format

nexthop { **ipv4** *ip-address* }

undo nexthop

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv4 *ip-address*	Specifies a next hop address for NQA test packets.	The value is in dotted decimal notation. **NOTE** The specified next hop must be the physical interface directly connected to the device that sends the NQA test packets.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario that an NQA test instance is associated with static routes, if a link becomes faulty, the NQA test instance detects this fault and then the static routes associated with the NQA test instance become Down. After the link recovers, the NQA test instance attempts to send ICMP test packets over the static routes. Because these static routes are still Down, the NQA test instance still fails to detect link connectivity. Traffic fails to be forwarded.

The **nexthop** command configures a next hop address for the NQA test packets, which ensures that the packets are forwarded when the link recovers from the fault, and the static routes associated with the NQA test instance are Up.

Prerequisites

Only the NQA ICMP test instance allows you to specify a next hop address for NQA test packets.

Precautions

After you specify the next hop address, you can also run the **source-interface** command to specify an outbound interface.

NOTE

If the next hop address is allocated dynamically using DHCP, the **source-interface** command must be run to specify the outbound interface.

In this case, the test must meet the following conditions. Otherwise, the test fails.

- The specified next hop address matches the outbound interface.
- The specified outbound interface cannot be the member interface of a logical interface.

Copyright © Huawei Technologies Co., Ltd.

Example

Configure a next hop address for NQA ICMP test packets.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test]  test-type icmp
[Huawei-nqa-user-test] nexthop ipv4 10.1.1.1
```

21.7.56 nqa

Function

The **nqa** command creates an NQA test instance and enters the NQA view.

The **undo nqa** command deletes an NQA test instance.

Format

nqa test-instance *admin-name test-name*

undo nqa { **test-instance** *admin-name test-name* | **all-test-instance** }

Parameters

Parameter	Description	Value
admin-name	Specifies the administrator of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters, excluding question marks (?), en dashes (-), a single or consecutive quotation marks (").
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters, excluding question marks (?), en dashes (-), a single or consecutive quotation marks (").
all-test-instance	Specifies all NQA test instances.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The NQA is an integrated network test function. NQA test instances can accurately detect network running status, collect test statistics, and reduce costs.

NQA measures the performance of different protocols running on the network. NQA allows enterprise users to collect network operation indexes in real time, such as total delay of the HTTP, TCP connection delay, DNS resolution delay, file transmission delay, FTP connection delay, and DNS resolution error ratio.

To check these performance indexes, you can create NQA test instances. The two ends of an NQA test are called the NQA client and NQA server. The NQA client is responsible for initiating an NQA test. After receiving packets, the NQA server sends response messages to the NQA client. You can learn about the running status of a corresponding network according to the returned packets.

Configuration Impact

After the **undo nqa all-test-instance** command is run, all NQA test instances including the running test instance will be deleted. In this scenario, you cannot perform any operation on each test instance.

Precautions

The **undo nqa test-instance** *admin-name test-name* command cannot delete a running NQA test instance.

The **undo nqa all-test-instance** command deletes all NQA test instances (including the running test instances).

Example

Create a test named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test]
```

Related Topics

21.7.95 test-type

21.7.57 nqa (NQA group view)

Function

The **nqa** command adds the specified NQA test instance to an NQA group.

The **undo nqa** command deletes the specified NQA test instance from an NQA group.

Format

nqa *admin-name test-name*

undo nqa *admin-name test-name*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
admin-name	Specifies the administrator of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters, excluding question marks (?), en dashes (-), a single or consecutive quotation marks (').
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters, excluding question marks (?), en dashes (-), a single or consecutive quotation marks (').

Views

NQA group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To add the specified NQA test instance to an NQA group, run the **nqa (NQA group view)** command. When an NQA group contains multiple NQA test instances, you can monitor multiple links at the same time by managing this NQA group.

The detection of an NQA group succeeds when at least one NQA test instance in the group succeeds. If no NQA test instance in an NQA group succeeds, the detection of this NQA group fails.

Precautions

If you delete an NQA test instance that belongs to an NQA group, this test instance is also deleted from this group.

Example

Add the NQA test instances **admin1 test1** and **admin2 test2** to the NQA group **group1**.

```
<Huawei> system-view
[Huawei] nqa-group group1
[Huawei-nqa-group-group1] nqa admin1 test1
[Huawei-nqa-group-group1] nqa admin2 test2
```

 Copyright © Huawei Technologies Co., Ltd.

21.7.58 nqa event

Function

The **nqa event** command associates an event with the NQA alarm.

The **undo nqa event** command deletes the configured event.

By default, no event is associated with the NQA alarm.

Format

nqa event *event-entry* { **log** | **trap** | **log-trap** | **linkage** *admin-name test-name* | **none** } [*description*]

undo nqa event [*event-entry*]

Parameters

Parameter	Description	Value
event-entry	Specifies the index of the entry in the event table.	The value is an integer that ranges from 1 to 65535.
log	Records a log for the event.	-
trap	Sends a trap to the NMS.	-
log-trap	Records a log and sends a trap to the NMS for the event.	-
linkage	Triggers a linkage test instance for the event.	-
admin-name	Specifies the administrator of the linkage test instance.	It is a string of 1 to 32 characters, spaces not supported. When quotation marks are used around the string, spaces are allowed in the string.
test-name	Specifies the name of the linkage test instance.	It is a string of 1 to 32 characters, spaces not supported. When quotation marks are used around the string, spaces are allowed in the string.
none	Marks as no event for the event.	-
description	Indicates the description of the event.	The value is a string of 1 to 127 characters with spaces supported.

Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the monitored item of an NQA test result exceeds the threshold, the system sends an alarm. The **nqa event** command can be used to associate an event with the alarm.

When an event occurs, you can process the event associated with the NQA alarm in the following ways:

- Record a log.
- Send a trap to the NMS.
- Record a log and send a trap to the NMS.
- Trigger a linkage test instance.
- Mark as no event.

Prerequisites

A test instance has been configured before associating it with an event. Creating other types of events requires no prerequisites.

Configuration Impact

After the **undo nqa event** command is run, all alarm events will be deleted if no event entry number is specified. If an event entry number is specified, the corresponding alarm event will be deleted.

Precautions

After running the **nqa event** command, run the **alarm** command to configure the alarm threshold for the monitored item of an NQA test result. In this case, an alarm is generated when the system becomes abnormal.

During configuration, check whether the event entry exists. If an event entry number to be entered exists, and the original event is not associated with an alarm, the original event which the event entry number corresponds to is overwritten after the event number is entered.

The event being associated with an alarm cannot be deleted.

Example

Associate event table 1 with linkage test instance **icmp**.

```
<Huawei> system-view
[Huawei] nqa event 1 linkage admin icmp
```

Related Topics

21.7.3 alarm

Copyright © Huawei Technologies Co., Ltd.

21.7.15 display nqa event
21.7.16 display nqa-event

21.7.59 nqa-ftp-record enable

Function

The **nqa-ftp-record enable** command enables the device to send the NQA test result to the FTP server using FTP.

The **undo nqa-ftp-record enable** command disables the device from sending the NQA test result to the FTP server using FTP.

By default, the test result is not sent to the FTP server using FTP.

Format

nqa-ftp-record enable

undo nqa-ftp-record enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The latest test result overrides the previous ones, because only a few NQA test results can be saved on the device. By default, the system stores the latest five test results. If you do not query the test results in a timely manner, some of them will be lost.

To solve this problem, you can save NQA test results to the FTP server using FTP. The NQA client sends test results to the specified FTP server using FTP. The FTP server then saves the test results to a text file.

Prerequisites

Parameters for the FTP connection have been set using the **nqa-ftp-record ip-address**, **nqa-ftp-record username**, **nqa-ftp-record password**, and **nqa-ftp-record filename** commands.

Precautions

During the FTP transmission, ensure the connectivity of the FTP connection.

 Copyright © Huawei Technologies Co., Ltd.

It is recommended that you use the FTP protocol in the secure network environment.

Example

Enable the device to send test results to the FTP server using FTP.

```
<Huawei> system-view
[Huawei] nqa-ftp-record enable
```

Related Topics

21.7.60 nqa-ftp-record filename
21.7.61 nqa-ftp-record ip-address
21.7.62 nqa-ftp-record item-num
21.7.63 nqa-ftp-record password
21.7.67 nqa-ftp-record username
21.7.65 nqa-ftp-record trap-enable
21.7.64 nqa-ftp-record time

21.7.60 nqa-ftp-record filename

Function

The **nqa-ftp-record filename** command configures a file name for NQA test results when the test results are saved to the FTP server.

The **undo nqa-ftp-record filename** command deletes the file name configured for NQA test results.

Format

nqa-ftp-record filename *filename*

undo nqa-ftp-record filename

Parameters

Parameter	Description	Value
filename	Specifies the file name.	The value is a string of 1 to 200 characters. The file name cannot end with any forward slashes (/) or backward slashes (\). **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The file to be saved is named in the format of file name-year-month-day-hour-minute-second.txt. If the number of sent results reaches the configured maximum value or the storage time of results expires, the system creates a file to save these results.

NOTE

Various FTP servers may support files with the file name in different length ranges. Before you configure this command, ensure that the target FTP server supports the length of the specified file name. Otherwise, NQA test results may fail to be transmitted using FTP.

Example

Save test results to the file named **a**.

```
<Huawei> system-view
[Huawei] nqa-ftp-record filename a
```

Related Topics

21.7.59 nqa-ftp-record enable
21.7.61 nqa-ftp-record ip-address
21.7.62 nqa-ftp-record item-num
21.7.63 nqa-ftp-record password
21.7.67 nqa-ftp-record username
21.7.64 nqa-ftp-record time

21.7.61 nqa-ftp-record ip-address

Function

The **nqa-ftp-record ip-address** command configures an IP address for the FTP server where NQA test results are saved.

The **undo nqa-ftp-record ip-address** command deletes the IP address of the FTP server where NQA test results are saved.

By default, no IP address is configured for the FTP server.

Format

nqa-ftp-record ip-address *ip-address*

undo nqa-ftp-record ip-address

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for the FTP server.	The IP address is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

During the FTP transmission, ensure the connectivity of the FTP connection. If the FTP connection fails and the buffer of the test result is full, the test result that is saved for the longest time in the buffer is deleted.

Example

Configure NQA test results to be sent to 10.1.1.8 using FTP.

```
<Huawei> system-view
[Huawei] nqa-ftp-record ip-address 10.1.1.8
```

Related Topics

21.7.59 nqa-ftp-record enable
21.7.60 nqa-ftp-record filename
21.7.62 nqa-ftp-record item-num
21.7.63 nqa-ftp-record password
21.7.67 nqa-ftp-record username
21.7.65 nqa-ftp-record trap-enable
21.7.64 nqa-ftp-record time

21.7.62 nqa-ftp-record item-num

Function

The **nqa-ftp-record item-num** command sets the number of test results that can be saved to a file on the FTP server.

The **undo nqa-ftp-record item-num** command restores the default number of test results that can be saved to a file on the FTP server.

By default, 100000 test results can be saved to a file on the FTP server.

Format

nqa-ftp-record item-num *item-number*

Copyright © Huawei Technologies Co., Ltd.

undo nqa-ftp-record item-num

Parameters

Parameter	Description	Value
item-number	Specifies the number of test results that can be saved to a file on the FTP server.	The value is an integer that ranges from 10000 to 2147483647.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When NQA test results are sent to the specified FTP server using FTP and the FTP server stores NQA test results to a text file, you need to set the maximum number of NQA test results that can be saved in each text file. If the number of test results exceeds the configured number, a new text file is created on the FTP server by the sequence number to store the subsequent NQA test results.

In addition, if the interval at which a test result is saved expires, a new file is also created on the FTP server by the sequence number to store NQA test results. If both the **nqa-ftp-record time** and **nqa-ftp-record item-num** commands are executed, a new file is created and the subsequent test results are saved to the new file when either of the interval at which a test result is saved or the number of test results reaches the configured value.

Configuration Impact

The system can send two test results to the FTP server each time. If the FTP server cannot resume the process of file writing after the process is interrupted, a new file is created on the FTP server to store NQA test results.

Before test results are sent to the FTP server using FTP, ensure that the FTP connection works properly.

Example

Set the number of NQA test results that can be saved to a file on the FTP server to 10010.

```
<Huawei> system-view
[Huawei] nqa-ftp-record item-num 10010
```

Related Topics

21.7.59 nqa-ftp-record enable

 Copyright © Huawei Technologies Co., Ltd.

21.7.61 nqa-ftp-record ip-address
21.7.60 nqa-ftp-record filename
21.7.63 nqa-ftp-record password
21.7.67 nqa-ftp-record username
21.7.64 nqa-ftp-record time

21.7.63 nqa-ftp-record password

Function

The **nqa-ftp-record password** command configures a password for logging in to the FTP server where NQA test results are saved.

The **undo nqa-ftp-record password** command deletes the password for logging in to the FTP server where NQA test results are saved.

Format

nqa-ftp-record password { *password* | **cipher** *cipher-password* }

undo nqa-ftp-record password

Parameters

Parameter	Description	Value
password	Specifies a password for logging in to the FTP server where NQA test results are saved.	The value is a string of 1 to 32 or 32 to 68 case-sensitive characters without spaces. • The length of a plaintext password ranges from 1 to 32. • The length of a ciphertext password ranges from 32 to 68. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher *cipher-password*	Specifies a password for logging in to the FTP server where NQA test results are saved.	The value is a string of 1 to 32 or 32 to 68 case-sensitive characters without spaces. • The length of a plaintext password ranges from 1 to 32. • The length of a ciphertext password ranges from 32 to 68. • If the password length is 32 and the configured ciphertext password can be decrypted successfully, the configured ciphertext password takes effect. If the configured ciphertext password cannot be decrypted, the plaintext password is used after passing the validity check. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command can be used when the system sends NQA test results to the specified FTP server using FTP. To ensure test security and prevent unauthorized users from accessing the network, you need to enable identity authentication. The **nqa-ftp-record password** command can be used to set the specified user and password. Only the user who enters the authorized user name and password is authorized to access the network.

Copyright © Huawei Technologies Co., Ltd.

Configuration Impact

Ensure that the **nqa-ftp-record password** command has been run before running the **nqa-ftp-record enable** command. Otherwise, FTP record (FTPR) cannot be enabled.

Precautions

The configured password and the user name configured by the **nqa-ftp-record username** command must be consistent.

Before test results are sent to the FTP server using FTP, ensure that the FTP connection works properly.

Example

Set the password for logging in to the FTP server to **Huawei-123**.

```
<Huawei> system-view
[Huawei] nqa-ftp-record password Huawei-123
```

Related Topics

21.7.59 nqa-ftp-record enable
21.7.60 nqa-ftp-record filename
21.7.62 nqa-ftp-record item-num
21.7.61 nqa-ftp-record ip-address
21.7.67 nqa-ftp-record username
21.7.64 nqa-ftp-record time

21.7.64 nqa-ftp-record time

Function

The **nqa-ftp-record time** command sets the interval at which test results are saved to a file on the FTP server.

The **undo nqa-ftp-record time** command restores the default interval at which test results are saved to a file on the FTP server.

By default, the interval at which NQA test results are saved to a file on the FTP server is 60 minutes.

Format

nqa-ftp-record time *time*

undo nqa-ftp-record time

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
time	Specifies the interval at which test results are stored to a text file using FTP.	The value is an integer that ranges from 1 to 43200, in minutes. The default value is 60.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When NQA test results are sent to a specified FTP server using FTP and the FTP server stores NQA test results to a text file, you need to set the interval at which test results are stored to a text file. A text file can store the test results in a specified period of time. If the interval exceeds the configured time, a new text file is created on the FTP server by the sequence number to store the subsequent NQA test results.

In addition, if the number of test results stored in a file on the FTP server reaches the configured number, a new file is also created on the FTP server by the sequence number to store the NQA test results. If both the **nqa-ftp-record time** and **nqa-ftp-record item-num** commands are configured, the following situations occur:

- If the number of test results stored in a file on the FTP server reaches the configured number, a new file is created and the subsequent test results is stored to the new file.
- If the number of test results stored in a file on the FTP server does not reach the configured number, but the interval at which a test result is stored reaches the configured interval, a new file is created and the subsequent test results are stored to the new file.

Precautions

Before test results are sent to the FTP server using FTP, ensure that the FTP connection works properly.

Example

Set the interval at which NQA test results are saved to 10 minutes.

```
<Huawei> system-view
[Huawei] nqa-ftp-record time 10
```

Related Topics

21.7.59 nqa-ftp-record enable

 Copyright © Huawei Technologies Co., Ltd.

21.7.60 nqa-ftp-record filename
21.7.62 nqa-ftp-record item-num
21.7.61 nqa-ftp-record ip-address
21.7.63 nqa-ftp-record password
21.7.67 nqa-ftp-record username

21.7.65 nqa-ftp-record trap-enable

Function

The **nqa-ftp-record trap-enable** command generates traps after NQA test results are saved using FTP.

The **undo nqa-ftp-record trap-enable** command disables the generation of traps after NQA test results are saved using FTP.

By default, no trap is generated when the NQA test result is saved using FTP.

Format

nqa-ftp-record trap-enable

undo nqa-ftp-record trap-enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command can be used when the system sends NQA test results to the specified FTP server using FTP. After the NQA test results are saved using FTP, the system sends a trap to the NMS.

Configuration Impact

If the test result is saved successfully at the first time, no trap is generated. If the test result is saved successfully at the second time, a trap is generated.

A trap is generated only after each text file is saved successfully. That is, when the number of saved test results reaches the configured number, or the interval at which a test result is saved reaches the configured time, the current text file can be saved successfully and a trap is generated.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Before test results are sent to the FTP server using FTP, ensure that the FTP connection works properly.

Example

Configure traps to be sent to the NMS using FTP after the NQA test result is saved.

```
<Huawei> system-view
[Huawei] nqa-ftp-record trap-enable
```

Related Topics

21.7.59 nqa-ftp-record enable

21.7.66 nqa-ftp-record source-address

Function

The **nqa-ftp-record source-address** command configures the address of the FTP client from which NQA test results are uploaded to the FTP server.

The **nqa-ftp-record source-address** restores the default FTP client address from which NQA test results are uploaded to the FTP server.

By default, the address of the FTP client from which NQA test results are uploaded to the FTP server is not configured.

Format

nqa-ftp-record source-address *ip-address*

undo nqa-ftp-record source-address

Parameters

Parameter	Description	Value
ip-address	Specifies an FTP client address.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To specify the address of the FTP client from which NQA test results are uploaded to the FTP server in a scenario that has client address restrictions, run the **nqa-ftp-record source-address** command.

Copyright © Huawei Technologies Co., Ltd.

Example

Configure 10.2.2.8 as the address of the FTP client from which NQA test results are uploaded to the FTP server.

```
<Huawei> system-view
[Huawei] nqa-ftp-record source-address 10.2.2.8
```

21.7.67 nqa-ftp-record username

Function

The **nqa-ftp-record username** command configures a user name for logging in to the FTP server where NQA test results are saved.

The **undo nqa-ftp-record username** command deletes the user name for logging in to the FTP server where NQA test results are saved.

By default, no user name is configured.

Format

nqa-ftp-record username *username*

undo nqa-ftp-record username

Parameters

Parameter	Description	Value
username	Specifies a user name for logging in to the FTP server where NQA test results are saved.	The value is a string of 1 to 255 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The user name configured for logging in to the FTP server where NQA test results are saved must be an existing user name on the FTP server.

Example

Set the user name for logging in to the FTP server to **ftp**.

```
<Huawei> system-view
[Huawei] nqa-ftp-record username ftp
```


Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.59 nqa-ftp-record enable
21.7.60 nqa-ftp-record filename
21.7.62 nqa-ftp-record item-num
21.7.61 nqa-ftp-record ip-address
21.7.63 nqa-ftp-record password

21.7.68 nqa-ftp-record vpn-instance

Function

The **nqa-ftp-record vpn-instance** command configures a VPN instance for the FTP server where NQA test results are saved.

The **undo nqa-ftp-record vpn-instance** command deletes the VPN instance configured for the FTP server where NQA test results are saved.

By default, the name of a VPN instance is not configured on the system.

Format

nqa-ftp-record vpn-instance *vpn-instance*

undo nqa-ftp-record vpn-instance

Parameters

Parameter	Description	Value
vpn-instance	Specifies the name of the VPN instance to which the FTP server belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command can be used when the system sends NQA test results to the specified FTP server using FTP. When the NQA client is connected to the FTP server through a VPN, the **nqa-ftp-record vpn-instance** command can be used to specify the name of the VPN instance.

Precautions

Copyright © Huawei Technologies Co., Ltd.

Before test results are sent to the FTP server using FTP, ensure that the FTP connection works properly.

Example

Configure VPN instance **v1** to send NQA test results.

```
<Huawei> system-view
[Huawei] nqa-ftp-record vpn-instance v1
```

Related Topics

21.7.59 nqa-ftp-record enable

21.7.60 nqa-ftp-record filename

21.7.62 nqa-ftp-record item-num

21.7.63 nqa-ftp-record password

21.7.67 nqa-ftp-record username

21.7.69 nqa-group

Function

The **nqa-group** command creates an NQA group and displays the NQA group view, or displays an existing NQA group view.

The **undo nqa-group** command deletes an NQA group.

Format

nqa-group *group-name*

undo nqa-group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of an NQA group.	It is a string of 1 to 32 case-sensitive characters without any space.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Copyright © Huawei Technologies Co., Ltd.

After an NQA group is created using the **nqa-group** command, you can add NQA test instances to the NQA group using the **nqa (NQA group view)** command, and then manage the NQA group to monitor multiple links at the same time.

Example

Create the NQA group **group1** and add the NQA test instances **admin1 test1** and **admin2 test2** to the NQA group.

```
<Huawei> system-view
[Huawei] nqa-group group1
[Huawei-nqa-group-group1] nqa admin1 test1
[Huawei-nqa-group-group1] nqa admin2 test2
```

21.7.70 nqa-jitter tag-version

Function

The **nqa-jitter tag-version** command sets the packet version for a jitter test instance.

The **undo nqa-jitter tag-version** command restores the default packet version for a jitter test instance.

By default, the packet version of a jitter test instance is 1.

Format

nqa-jitter tag-version *version-number*

undo nqa-jitter tag-version

Parameters

Parameter	Description	Value
version-number	Specifies the packet version for a jitter test instance.	The value can be 1 or 2.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Version 1 does not support unidirectional packet loss statistics.

Version 2 produces more accurate packet statistics, which helps network administrators to locate network faults and detect malicious attacks towards the

Copyright © Huawei Technologies Co., Ltd.

network. After version 2 and collecting the packet loss across a unidirectional link are enabled, you can view the packet loss across the link from the source end to the destination end, from the destination end to the source end, or in an unknown direction in the test results.

Therefore, configuring version 2 is recommended.

Configuration Impact

If the packet version of a jitter test instance has been configured, running the **nqa-jitter tag-version** command will override the previous configuration.

Precautions

- If the packet version for the jitter test is 1, configuring the UDP server is optional.
- If the packet version of the jitter test is 2, configuring UDP server is mandatory. You need to run the **nqa-server udpecho** command to configure the UDP server. If the command is not configured, the UDP jitter test instance on the ingress will fail due to timeout.

Example

Set the packet version of a jitter test instance to 2.

```
<Huawei> system-view
[Huawei] nqa-jitter tag-version 2
```

21.7.71 nqa-server rtp-udp

Function

The **nqa-server rtp-udp** command configures an RTP server for an NQA test.

The **undo nqa-server rtp-udp** command deletes the RTP server for an NQA test.

By default, no RTP server is configured.

Format

nqa-server rtp-udp [**vpn-instance** *vpn-instance-name*] *ip-address port-number*

undo nqa-server rtp-udp { [**vpn-instance** *vpn-instance-name*] *ip-address port-number* | **all** }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the RTP server belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ip-address	Specifies the IP address of the RTP server for monitoring RTP services.	The value is in dotted decimal notation.
port-number	Specifies the port number of the RTP server for monitoring RTP services.	The value is an integer that can be any value in the range of 1025 to 65535.
all	Specifies RTP servers for all NQA tests.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Incomplete or unclear pictures may occur during a Telepresence conference because of the unstable network. You can deploy an RTP test instance at the source node, and run the **nqa-server rtp-udp** command at the transit mode and destination node to deploy RTP servers to perform a jitter test. This method helps you easily locate faults, facilitates network maintenance, and improves Telepresence conference experience.

Example

Configure an RTP UDP server for an NQA test instance.

```
<Huawei> system-view
[Huawei] nqa-server rtp-udp 10.10.10.2 2500
```

21.7.72 nqa-server session-record enable

Function

The **nqa-server session-record enable** command enables NQA client information display on the NQA server.

The **undo nqa-server session-record enable** command disables NQA client information display on the NQA server.

By default, NQA client information display is disabled on the NQA server.

Format

nqa-server session-record enable

undo nqa-server session-record enable

Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **nqa-server session-record enable** command is executed on the NQA server to enable NQA client information display, run the **display nqa-server session** command to view information about all NQA clients connected to the NQA server. The NQA client information includes the IP address of NQA server, IP address of NQA client, source port of NQA client, and VPN.

Precautions

This command is valid for only hardware-based UDP jitter test.

Example

Enable NQA client information display on the NQA server.

```
<Huawei> system-view
[Huawei] nqa-server session-record enable
```

Related Topics

21.7.26 display nqa-server session

21.7.73 nqa-server tcpconnect

Function

The **nqa-server tcpconnect** command configures the IP address and port number for the TCP server in an NQA TCP test instance.

The **undo nqa-server tcpconnect** command deletes the IP address and port number configured for the TCP server in an NQA TCP test instance.

By default, no IP address or port number is configured for the TCP server in an NQA TCP test instance.

Format

nqa-server tcpconnect [**vpn-instance** *vpn-instance-name*] *ip-address port-number*

undo nqa-server tcpconnect { **all** | [**vpn-instance** *vpn-instance-name*] *ip-address port-number* }

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the TCP server belongs. **NOTE** This parameter is invalid when a loopback address is specified as the TCP server address.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Indicates all TCP listening addresses and port numbers.	-
ip-address	Specifies the IP address of the TCP server for monitoring TCP services.	The value is in dotted decimal notation.
port-number	Specifies the port number of the TCP server for monitoring TCP services.	The value is an integer that ranges from 1 to 65535. The configured port cannot be a well-known port or used by other modules.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The NQA TCP test is used to detect the rate at which a TCP connection is set up between an NQA client and a TCP server through the three-way handshake. In a TCP test instance, a TCP server needs to be configured on the server end to respond to probe packets.

Perform the following steps on the client to configure TCP server parameters:

- Run the **destination-address** command to configure the destination address of an NQA test instance or the IP address of the TCP server.

Copyright © Huawei Technologies Co., Ltd.

- Run the **destination-port** command to configure the destination port number of an NQA test instance, or the port number of the TCP server.

If the client and the server are connected through a VPN, you need to specify the VPN instance name.

Configuration Impact

Running the **undo nqa-server tcpconnect all** command will delete the IP address and port number of the TCP server.

Precautions

A TCP server is configured only in a TCP test instance.

Example

Create a TCP server for an NQA test instance with the IP address as 10.10.10.1 and the port number as 5000.

```
<Huawei> system-view
[Huawei] nqa-server tcpconnect 10.10.10.1 5000
```

Related Topics

21.7.9 destination-address

21.7.10 destination-port

21.7.74 nqa-server udpecho

Function

The **nqa-server udpecho** command configures the IP address and port number for the UDP server in an NQA test.

The **undo nqa-server udpecho** command deletes the IP address and port number configured for the UDP server in an NQA test.

By default, no IP address or port number is configured for the UDP server in an NQA test.

Format

nqa-server udpecho [**vpn-instance** *vpn-instance-name*] { **auto-address** | *ip-address* | **ipv6** *ipv6-address* } *port-number*

undo nqa-server udpecho { [**vpn-instance** *vpn-instance-name*] { **auto-address** | *ip-address* | **ipv6** *ipv6-address* } *port-number* | **all** }

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the server belongs. **NOTE** This parameter is invalid when a loopback address is specified as the UDP server address.	The value is a string of 1 to 31 characters.
all	Specifies a server for all NQA test instances.	-
ip-address	Specifies the IP address of the server for monitoring UDP services.	The value is in dotted decimal notation.
port-number	Specifies the port number of the server for monitoring UDP services.	The value is an integer that ranges from 1 to 65535. The configured port cannot be a well-known port or used by other modules.
ipv6 *ipv6-address*	Specifies the IPv6 address of the server for monitoring UDP services.	-
auto-address	Configures the UDP service on the NQA server to automatically monitor all IPv4 addresses.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a UDP server.

UDP packets are transmitted in a jitter test. The test is used to obtain the packet delay, jitter, and packet loss ratio by comparing timestamps in the request and response packets. A UDP server needs to be configured for an NQA test to respond to probe packets.

If the client and the server are connected through a VPN, you need to specify the VPN instance name.

If the local IPv4 address cannot be predicted because of dynamic address allocation by DHCP, specify the **auto-address** keyword to configure the UDP service on the NQA server to automatically monitor all IPv4 addresses.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Impact

Running the **undo nqa-server udpecho all** command will delete the IP address and port number of the UDP server for all NQA UDP test instances.

Precautions

- If the version number of the jitter test packets is 1, the command is optional.
- If the version number of the jitter test packets is 2, the command is mandatory. If the command is not configured, the jitter test instance on the ingress will fail due to timeout.

Example

Create an NQA UDP monitoring server with the IP address 10.10.10.2 and the port number 6000.

```
<Huawei> system-view
[Huawei] nqa-server udpecho 10.10.10.2 6000
```

21.7.75 nqa upload statistics datetime-type

Function

The **nqa upload statistics datetime-type** command configures the time type based on which NQA test results are uploaded to the server.

The **undo nqa upload statistics datetime-type** command restores the default time type based on which NQA test results are uploaded to the server.

The default time type based on which NQA test results are uploaded to the server is Coordinated Universal Time (UTC).

Format

nqa upload statistics datetime-type { **utc** | **local** }

undo nqa upload statistics datetime-type

Parameters

Parameter	Description	Value
utc	Indicates that NQA test results are uploaded to the server based on UTC.	-
local	Indicates that NQA test results are uploaded to the server based on local time.	-

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

UTC is the default time type based on which NQA test results are uploaded to the server. This time type causes difficulties in time understanding. To change the time type to local time, run the **nqa upload statistics datetime-type local** command.

NOTE

- UTC: Coordinated Universal Time, which is the standard time used globally.
- Local time: If the local time is faster than UTC, for example, Beijing Time is 8 hours faster than UTC, the time zone of China is UTC+8. If the local time is slower than UTC, for example, Hawaii Time is 10 hours slower than UTC, the time zone of Hawaii is UTC-10.

Example

Change the time type based on which NQA test results are uploaded to the server to local time.

```
<Huawei> system-view
[Huawei] nqa upload statistics datetime-type local
```

21.7.76 probe-count

Function

The **probe-count** command sets the number of probes for an NQA test instance.

The **undo probe-count** command restores the default number of probes for an NQA test instance.

By default, the number of probes for an NQA test instance is 3.

Format

probe-count *number*

undo probe-count

Parameters

Parameter	Description	Value
number	Specifies the number of probes in an NQA test instance.	The value is an integer that ranges from 1 to 15. The default value is 3. **NOTE** The number of probes in a trace test instance cannot be more than 10.

Copyright © Huawei Technologies Co., Ltd.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An NQA test consists of multiple probes. By default, if one or more probes are successful in an NQA test, the test is considered successful. If all probes fail, the test is considered a failure. The number of probes in an NQA test is based on the network quality.

- If the network to be tested is a reliable network, the number of probes can be set relatively small because the probe can be successful after a small number of probe packets are sent.
- If the network to be tested is an unreliable network, the number of probes can be set relatively large because the probe can be successful only after a large number of probe packets are sent.

You can also detect the network quality based on statistics obtained from multiple probes. For example,

- If the probe test is successful after a small number of probes packets are sent, the network quality is good.
- If the probe test is successful after a large number of probes packets are sent, the network quality is poor.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Configuration Impact

- In jitter test instances, the number of sent packets = **probe-count** x **jitter-packetnum**, but the product cannot exceed 3000.
- If the number of probes has been configured, running the **probe-count** command will override the previous configuration.

Precautions

The number of probes cannot be set for an FTP or a DNS test.

The number of probes of a running test instance cannot be changed.

Example

Set the number of probes to 6 in NQA test instance **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] probe-count 6
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.47 jitter-packetnum
21.7.77 probe-failtimes

21.7.77 probe-failtimes

Function

The **probe-failtimes** command sets the threshold for the number of traps to be sent when the NQA test fails. That is, test packet fragmentation is not allowed.

The **undo probe-failtimes** command restores the default threshold for the number of traps to be sent when the NQA test fails.

By default, one trap is sent for each probe failure.

Format

probe-failtimes *times*

undo probe-failtimes

Parameters

Parameter	Description	Value
times	Specifies the threshold for the number of traps to be sent when the NQA test fails, that is, the number of continuous probe failures.	The value is an integer that ranges from 1 to 15. The default value is 1.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The NQA probe test is used to check whether response packets are received in a probe. If the number of continuous probe failures reaches the specified value, the system sends a trap to the specified NMS.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Follow-up Procedure

Copyright © Huawei Technologies Co., Ltd.

Run the **send-trap probefailure** command to enable the system to send a trap to the NMS after a probe fails. Otherwise, the trap cannot be sent to the NMS after a probe fails.

Precautions

- This configuration of a running test instance cannot be changed.
- If the test instance does not support **probe-count** *number*, you are advised to set **probe-failtimes** to 1; otherwise, traps cannot be sent.
- If the test instance supports **probe-count** *number*, you are advised to set **probe-failtimes** to be smaller or equivalent to probe-count; otherwise, traps cannot be sent.

Example

Set the number of continuous probe failures to 10 in the test named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type tcp
[Huawei-nqa-user-test] probe-failtimes 10
```

Related Topics

21.7.95 test-type

21.7.86 send-trap

21.7.78 packet-rewrite-check

Function

The **packet-rewrite-check** command configures the NQA packet rewrite check function by padding NQA packets.

The **undo packet-rewrite-check** command cancels NQA packet padding.

By default, NQA packet padding is not configured.

Format

packet-rewrite-check { **alternant-binary** | **same-binary** }

undo packet-rewrite-check

Parameters

Parameter	Description	Value
alternant-binary	Pads bits 0101 and 1010 alternatively into test packets.	-
same-binary	Pads bits 0000 and 1111 alternatively into test packets.	-

Views

NQA view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packet rewrite frequently occurs on the live network. The NQA packet rewrite check function can locate the device where the packet rewrite occurs by dividing the network into different parts and checking these parts one by one. The NQA packet rewrite check function uses test packets padded with specified bits for rewrite checking. Bit transition may occur on any bit of the packet, for example, it may occur on one bit in bits 1010, 0000, or 1111. To locate where the bit transition or whether packet rewrite occurs, configuring both **alternant-binary** and **same-binary** is recommended. In this manner, the length and contents of the bits can be changed as required. For example, bits 1010 can be padded into the first test packet and 0101 into the second one. After receiving the response packet, the device checks contents of the packet and determines whether the packet is rewritten.

Configuration Impact

Packet contents will be changed because bit characters are padded into the packet.

Precautions

If the **packet-rewrite-check** command has been configured, the **datafill** command cannot be used. In addition, you cannot configure the **hardware-based enable** command, because the LPU does not support the NQA packet rewrite check function.

Example

Pad bits 0000 and 1111 alternatively into test packets to be sent in the test instance named **user city1**.

```
<Huawei> system-view
[Huawei] nqa test-instance user city1
[Huawei-nqa-user-city1] test-type jitter
[Huawei-nqa-user-city1] packet-rewrite-check same-binary
```

21.7.79 records

Function

The **records** command sets the maximum number of history records and the maximum number of test results for NQA test instances.

The **undo records** command restores the default maximum number of history records and the default maximum number of test results for NQA test instances.

By default, the number of history records is 50, and the number of test results is 5.

Copyright © Huawei Technologies Co., Ltd.

Format

records { **history** *number* | **result** *number* }

undo records { **history** | **result** }

Parameters

Parameter	Description	Value
history *number*	Specifies the maximum number of history records.	The value is an integer that ranges from 0 to 50. The default value is 50.
result *number*	Specifies the maximum number of test results.	The value is an integer that ranges from 1 to 10. The default value is 5.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **records** command to set the maximum number of history records and the maximum number of test results for NQA test instances.

By default, a test instance supports 50 history records. You need to limit the number of history records on the device. In addition, you need to set the number of allowed remaining history records that can be added. The configured maximum number of history records cannot exceed the sum of the total default number of history records and the remaining number of history records.

Precautions

The type of a test instance has been specified using the **test-type** command.

This configuration of a running test instance cannot be changed.

Example

Set the maximum number of history records to 30 for test instance **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] records history 30
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.18 display nqa history
21.7.20 display nqa results

21.7.80 records history-filter

Function

The **records history-filter** command enables a device to filter out records in a historical NQA test instance table.

The **undo records history-filter** command disables a device from filtering records in historical NQA test instance tables.

By default, a device does not filter records in historical NQA test instance tables.

Format

records history-filter { **all** | **failures** }

undo records history-filter

Parameters

Parameter	Description	Value
all	Indicates all records.	-
failures	Indicates records about failed test instances.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Before running the **records history-filter** command, you must run the **test-type** command to specify the test instance type.

To filter records about failed NQA test instances, configure the **failures** parameter in the **records history-filter** command.

NOTE

The **records history-filter** command only takes effect on ICMP test instances.

Example

Enable a device to filter records about failed NQA test instances in a test named **user test**.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] records history-filter failures
```

Related Topics

21.7.18 display nqa history

21.7.20 display nqa results

21.7.81 remote-pw-id

Function

Using the **remote-pw-id** command, you can configure the ID of the remote end of a PW or a VC.

Using the **undo remote-pw-id** command, you can remove the configured ID of the remote end of a PW or a VC.

When the VC type is LDP, **remote-pw-id** defaults to be 0.

Format

remote-pw-id *remote-pw-id*

undo remote-pw-id

Parameters

Parameter	Description	Value
remote-pw-id	Specifies the ID of the remote end of a PW or a VC.	The value is a decimal integer. • In the case of a PWE3 ping test instance, the value of *remote-pw-id* is an integer that ranges from 1 to 4294967295, and only the VC type of LDP is supported. The default value is 0, indicating that the ID of the remote end of a PW is not configured. • In the case of a PWE3 trace, – if the VC type is LDP, the value of *remote-pw-id* is an integer that ranges from 1 to 4294967295. The default value is 0. – if the VC type is BGP, the value of *remote-pw-id* is an integer that ranges from 0 to 65534.

Views

NQA view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Before running the **remote-pw-id** command, you must set the test type to PWE3 Trace or PWE3 Ping in the NQA view.

Example

In the NQA view, configure the ID of the remote end of a PW to 100, the administrator to admin, and the test type to PWE3 trace.

```
<Huawei> system-view
[Huawei] nqa test-instance admin pwe3
[Huawei-nqa-admin-pwe3] test-type pwe3trace
[Huawei-nqa-admin-pwe3] remote-pw-id 100
```

21.7.82 remote-address (NQA view)

Function

Using the **remote-address** command, you can configure the remote address.

Using the **undo remote-address** command, you can delete a remote address.

By default, no remote address is configured.

Format

remote-address ipv4 *remote-ip-address*

undo remote-address

Parameters

Parameter	Description	Value
ipv4 *remote-ip-address*	Specifies the remotely assigned IP address.	It is in dotted decimal notation.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Use the **remote-address** command, you can specify a remote ip address.

Copyright © Huawei Technologies Co., Ltd.

The supported test instance are:

- vplsmtrace
- vplspwping

Example

Configure an IP address 1.1.1.1 for VPLS multicast trace test.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type vplsmtrace
[Huawei-nqa-user-test] remote-address ipv4 1.1.1.1
```

21.7.83 reset ip nqa-compatible responder statistics

Function

The **reset ip nqa-compatible responder statistics** command deletes statistics on the NQA handshake packets sent from the third-party device or NMS software.

Format

reset ip nqa-compatible responder statistics

Parameters

None

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Before checking the latest status of communication between the device and third-party device or NMS software, use this command to delete old statistics first.

Precautions

Once statistics on the NQA handshake packets sent from the third-party device or NMS software are deleted, they cannot be restored. Confirm the action before you perform it.

Example

Delete statistics on NQA handshake packets sent from the third-party device or NMS software.

```
<Huawei> reset ip nqa-compatible responder statistics
```

 Copyright © Huawei Technologies Co., Ltd.

21.7.84 restart (NQA view)

Function

The **restart** command restarts the current running test instance.

Format

restart

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Function of the **restart** command is the same as that of the **start now** command.

Example

Restart the test instance named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] destination-port 8000
[Huawei-nqa-user-test] destination-address ipv4 10.1.1.1
[Huawei-nqa-user-test] restart
```

Related Topics

21.7.92 start

21.7.93 stop

21.7.85 sendpacket passroute

Function

The **sendpacket passroute** command enables test packets to be sent without searching the routing table.

The **undo sendpacket passroute** command restores the default setting.

By default, the test packet is sent according to the routing table.

Copyright © Huawei Technologies Co., Ltd.

Format

sendpacket passroute

undo sendpacket passroute

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The type of a test instance has been specified using the **test-type** command. The type of test instances that are supported is as follows:

- ICMP
- TCP
- UDP
- HTTP
- Jitter
- FTP
- SNMP
- Trace

You cannot change this configuration of a running test instance.

After the **sendpacket passroute** command is executed, the device sends test packets without searching the routing table. However, the configurations of **ttl** and **ip-forwarding** become invalid.

Example

Enable test packets to be sent without searching the routing table.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] sendpacket passroute
```

Related Topics

21.7.95 test-type

21.7.56 nqa

Copyright © Huawei Technologies Co., Ltd.

21.7.86 send-trap

Function

The **send-trap** command configures conditions for sending traps.

The **undo send-trap** command deletes the previous configuration.

By default, the device is disabled from sending traps.

Format

send-trap { **all** | { **owd-ds** | **owd-sd** | **probefailure** | **rtd** | **testcomplete** | **testfailure** | **jitter-sd** | **jitter-ds** | **testresult-change** } * }

undo send-trap { **all** | { **owd-ds** | **owd-sd** | **probefailure** | **rtd** | **testcomplete** | **testfailure** | **jitter-sd** | **jitter-ds** | **testresult-change** } * }

Parameters

Parameter	Description	Value
all	Indicates that a trap is sent in any of the following situations: ● The one-way delay (OWD) exceeds the threshold. ● The RTD exceeds the threshold. ● NQA probes fail. ● An NQA test succeeds. ● NQA tests fail. ● NQA probe result changes.	-
owd-ds	Indicates that a trap is sent when the OWD from the destination to the source exceeds the threshold. **NOTE** This parameter applies only to jitter test instances.	-
owd-sd	Indicates that a trap is sent when the OWD from the source to the destination exceeds the threshold. **NOTE** This parameter applies only to jitter test instances.	-
probefailure	Indicates that a trap is sent when the number of probe failures reaches the threshold. **NOTE** This parameter does not apply to Jitter test instances.	-
rtd	Indicates that a trap is sent when the RTD exceeds the threshold.	-
testcomplete	Indicates that a trap is sent when a test succeeds.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
testfailure	Indicates that a trap is sent when the number of test failures reaches the threshold.	-
jitter-sd	Indicates that a trap is sent when the jitter from the source to the destination exceeds the threshold.	-
jitter-ds	Indicates that a trap is sent when the jitter from the destination to the source exceeds the threshold.	-
testresult-change	Indicates that a trap is sent when the probe result changes. **NOTE** This function supports only ICMP test instances.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traps are generated no matter whether the NQA test succeeds or fails. You can determine whether traps are sent to the NMS by enabling or disabling the trap function.

The device sends traps to the NMS in any of the following situations:

- The OWD exceeds the threshold.

  If the OWD from the source to the destination or from the destination to the source exceeds the threshold, the device sends a trap to the NMS using the configured NMS address.
- The RTD exceeds the threshold.

  If the RTD exceeds the threshold, the device sends a trap to the NMS using the configured address.
- NQA probes fail.

  When no response packet is received after a specified number of continuous test packets are sent, the device sends a trap to the NMS using the configured address.
- An NQA test succeeds.

  When the device receives a response packet from a destination address, the device sends a trap to the NMS using the configured address.
- NQA tests fail.

  When the number of continuous test failures reaches the maximum number, the device sends a trap to the NMS using the configured address.
- NQA probe result changes.

 Copyright © Huawei Technologies Co., Ltd.

When the NQA probe result changes, the device sends a trap to the NMS using the configured address.

You can run the **send-trap** command to configure conditions for sending traps. When a condition is met, the device sends a trap to the NMS.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

The route between the device and NMS is reachable, and related configurations are complete. The trap function has been enabled for the NQA module using the **snmp-agent trap enable feature-name nqa** command, and the host where traps are sent is configured using the **snmp-agent target-host trap-hostname** command; otherwise, traps cannot be sent to the NMS.

Precautions

You cannot change this configuration of a running test instance.

Example

Configure the test instance **user test** to send a trap when the test fails.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] send-trap testfailure
```

Related Topics

21.7.95 test-type
21.7.88 snmp-agent trap enable feature-name nqa
21.1.27 snmp-agent target-host trap-hostname
21.7.77 probe-failtimes
21.7.94 test-failtimes

21.7.87 set-df

Function

The **set-df** command configures the DF (Don't Fragment) field of the test packet. This field prevents packets from being fragmented.

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

By default, packet fragmentation is allowed.

Format

set-df

undo set-df

Parameters

None

Copyright © Huawei Technologies Co., Ltd.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If two hosts need to communicate with each other over multiple networks, the smallest MTU value of the networks is the path MTU value. Packets can be transmitted normally over multiple networks only after the path MTU value is obtained.

If the DF bit of a packet is not configured, and the length of the packet is longer than the MTU value, the packet will be fragmented into several fragments that are shorter than the path MTU value. As a result, the path MTU cannot be detected by sending packets with increasing lengths. To detect the path MTU value, run the **set-df** command to prohibit packet fragmentation. Then, increase the length of packets sent along the path to find the path MTU value.

Prerequisites

The type of a test instance has been set to Trace using the **test-type trace** command.

Precautions

The configuration of the DF bit for packets in a running test instance cannot be changed.

Example

Set the test packet sent without being fragmented.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type trace
[Huawei-nqa-user-test] set-df
```

Related Topics

21.7.95 test-type

21.7.88 snmp-agent trap enable feature-name nqa

Function

The **snmp-agent trap enable feature-name nqa** command enables the trap function for the NQA module.

The **undo snmp-agent trap enable feature-name nqa** command disables the trap function for the NQA module.

By default, the trap function is enabled for the NQA module.

Copyright © Huawei Technologies Co., Ltd.

Format

snmp-agent trap enable feature-name nqa [**trap-name** { **nqaresultsprobefailed** | **nqahttpstatsprobefailed** | **pingprobefailed** | **nqaftpstatsprobefailed** | **pingtestfailed** | **pingtestcompleted** | **traceroutetestfailed** | **traceroutetestcompleted** | **nqaresultstestfailed** | **nqaresultstestcompleted** | **nqaresultsthresholdnotification** | **nqahttpstatstestfailed** | **nqahttpstatstestcompleted** | **nqahttpstatsthresholdnotification** | **nqaftpstatstestfailed** | **nqaftpstatstestcompleted** | **nqaftpstatsthresholdnotification** | **nqajitterstatstestfailed** | **nqajitterstatstestcompleted** | **nqajitterstatsrtdthresholdnotification** | **nqajitterstatsowdthresholdnotificationsd** | **nqajitterstatsowdthresholdnotificationds** | **nqarisingalarmnotification** | **nqafaillingalarmnotification** | **nqaftpsaverecordnotification** | **nqajitterstatsjitterthresholdnotificationsd** | **nqajitterstatsjitterthresholdnotificationds** | **nqareflectorstatechangenotification** | **nqaResultsTestResultChange** }]

undo snmp-agent trap enable feature-name nqa [**trap-name** { **nqaresultsprobefailed** | **nqahttpstatsprobefailed** | **pingprobefailed** | **nqaftpstatsprobefailed** | **pingtestfailed** | **pingtestcompleted** | **traceroutetestfailed** | **traceroutetestcompleted** | **nqaresultstestfailed** | **nqaresultstestcompleted** | **nqaresultsthresholdnotification** | **nqahttpstatstestfailed** | **nqahttpstatstestcompleted** | **nqahttpstatsthresholdnotification** | **nqaftpstatstestfailed** | **nqaftpstatstestcompleted** | **nqaftpstatsthresholdnotification** | **nqajitterstatstestfailed** | **nqajitterstatstestcompleted** | **nqajitterstatsrtdthresholdnotification** | **nqajitterstatsowdthresholdnotificationsd** | **nqajitterstatsowdthresholdnotificationds** | **nqarisingalarmnotification** | **nqafaillingalarmnotification** | **nqaftpsaverecordnotification** | **nqajitterstatsjitterthresholdnotificationsd** | **nqajitterstatsjitterthresholdnotificationds** | **nqareflectorstatechangenotification** | **nqaResultsTestResultChange** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap function for the specified event for the NQA module.	-
nqaresultsprobefailed	Sends a trap when the number of continuous probe failures exceeds the threshold.	-
nqahttpstatsprobefailed	Sends a trap when the number of continuous probe failures exceeds the threshold in an HTTP test instance.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pingprobefailed	Sends a trap when the number of continuous ping failures exceeds the threshold.	-
nqaftpstatsprobefailed	Sends a trap when a test result fails to be saved to the FTP server.	-
pingtestfailed	Sends a trap when a ping test fails.	-
pingtestcompleted	Sends a trap when a ping test is complete.	-
traceroutetestfailed	Sends a trap when no destination path is obtained in a traceroute test.	-
traceroutetestcompleted	Sends a trap when a destination path is obtained in a traceroute test.	-
nqaresultstestfailed	Sends a trap when a common test fails.	-
nqaresultstestcompleted	Sends a trap when a common test is complete.	-
nqaresultsthresholdnotification	Sends a trap when the completing time of a test instance expires.	-
nqahttpstatstestfailed	Sends a trap when an HTTP test fails.	-
nqahttpstatstestcompleted	Sends a trap when an HTTP test is complete.	-
nqahttpstatsthresholdnotification	Sends a trap when the completing time of an HTTP test instance expires.	-
nqaftpstatstestfailed	Sends a trap when an FTP test fails.	-
nqaftpstatstestcompleted	Sends a trap when an FTP test is complete.	-
nqaftpstatsthresholdnotification	Sends a trap when the completing time of an FTP test instance expires.	-
nqajitterstatstestfailed	Sends a trap when a jitter test fails.	-
nqajitterstatstestcompleted	Sends a trap when a jitter test is complete.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
nqajitterstatsrtdthresholdnotification	Sends a trap when the completing time of a jitter test instance expires.	-
nqajitterstatsowdthresholdnotificationsd	Sends a trap when the time from the source to the destination expires in a jitter test instance.	-
nqajitterstatsowdthresholdnotificationds	Sends a trap when the time from the destination to the source expires in a jitter test instance.	-
nqarisingalarmnotification	Sends a traps when the value of the monitored node exceeds the threshold.	-
nqafaillingalarmnotification	Sends a traps when the value of the monitored node is smaller than the threshold.	-
nqaftpsaverecordnotification	Sends a trap when a test result is saved to the FTP server.	-
nqajitterstatsjitterthresholdnotificationsd	Sends a trap when the jitter time from the source to the destination expires in a jitter test instance.	-
nqajitterstatsjitterthresholdnotificationds	Sends a trap when the jitter time from the destination to the source expires in a jitter test instance.	-
nqareflectorstatechangenotification	Trap generated when the reflector status in the general flow test instance changes.	-
nqaResultsTestResultChange	Trap generated when the probe result of an ICMP test instance changes.	-

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To enable the trap function for one or more specific events, specify **trap-name**.

Example

Enable the trap function for the NQA nqaftpstatsprobefailed module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name nqa trap-name nqaftpstatsprobefailed
```

Related Topics

21.7.27 display snmp-agent trap feature-name nqa all

21.7.89 source-address

Function

The **source-address** command sets the source IP address for a test instance.

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

By default, the IP address of the interface where packets are sent functions as the source IP address of a test instance.

Format

source-address { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* }

undo source-address

Parameters

Parameter	Description	Value
ipv4 *ipv4-address*	Specifies the IPv4 source address for the NQA test instance.	The value is in dotted decimal notation.
ipv6 *ipv6-address*	Specifies the IPv6 source address for the NQA test instance. **NOTE** Only DNS, ICMP, trace, and jitter tests support IPv6 source addresses.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Views

NQA view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **source-address** command is used to configure the source IP address for the NQA test. After the test packets reach the destination, a packet is returned, with the configured source IP address as the destination address. If no source IP address is configured, the system specifies the IP address that sends test packets as the source IP address.

Prerequisites

The type of a test instance has been specified using the **test-type** command. However, the test type cannot be DHCP.

Precautions

The configuration of the source IP address of the running test instance cannot be changed.

Example

Set the source IP address to 10.1.1.1 for test instance **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] source-address ipv4 10.1.1.1
```

Related Topics

21.7.95 test-type

21.7.90 source-interface

21.7.91 source-port

21.7.90 source-interface

Function

The **source-interface** command configures the source interface for an NQA test instance.

The **undo source-interface** command cancels the configuration.

By default, no source interface is configured for an NQA test instance.

Format

source-interface *interface-type interface-number*

undo source-interface

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the source interface for an NQA test instance.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After test packets reach the destination address, the destination end sends response packets to the client end. After the **source-interface** command is used to configure the source interface for an NQA test instance, there are the following scenarios:

- If the **source-address** command is run to specify the source IP address, the test packets are sent from the specified source interface, but the response packets are received from the configured source IP address.
- If no source IP address is specified for an NQA test instance, the IP address of the source interface will be used as the source IP address of the NQA test instance. In this scenario, the initiated and responded packets are both transmitted over the outbound interface specified by the **source-interface** command.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The source interface can be configured only for DHCP, ICMP, and Jitter test instances.

Precautions

The configuration of the source interface of a running test instance cannot be changed.

Use an interface with an IP address as the source interface of the NQA test instance; otherwise, the command does not take effect.

In the load balancing scenario, trunks and their member interfaces do not support tests.

Example

Set the source interface of test instance **user test** to gigabitethernet 1/0/0.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] source-interface gigabitethernet 1/0/0
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.95 test-type
21.7.91 source-port
21.7.89 source-address

21.7.91 source-port

Function

The **source-port** command configures the source port for an NQA test instance.

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

No default source port number is specified, port numbers are randomly allocated by the system.

Format

source-port *port-number*

undo source-port

Parameters

Parameter	Description	Value
port-number	Specifies the source port number for an NQA test instance.	The value is an integer that ranges from 1 to 65535. The configured port cannot be a well-known port or used by other modules.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a source port number is specified in an NQA test instance, NQA test packets can be regulated more accurately, which prevents the probe packets from being filtered by rules such ACL. The **source-port** command can be used to configure the source port for this NQA test instance:

- If no source port number is specified for an NQA test instance, a port number is selected at random to receive or send NQA test packets.
- If source port number is specified for an NQA test instance, the specified port number is used to receive and send NQA test packets.

Prerequisites

Copyright © Huawei Technologies Co., Ltd.

The test instance type has been specified using the **test-type** command. The source port number can be configured only for TCP, FTP, HTTP, UDP, jitter (including jitter test instances based on the mechanism that the LPU sends packets), and SNMP test instances.

Precautions

The port specified in the **source-port** command must be available; otherwise, the probe fails.

Port numbers 61442 to 65535 are reserved. Do not use the port numbers; otherwise, the probe fails.

You cannot change this configuration of a running test instance.

Example

Set the source port number of test instance **user test** to 3000.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type tcp
[Huawei-nqa-user-test] source-port 3000
```

Related Topics

21.7.95 test-type

21.7.90 source-interface

21.7.89 source-address

21.7.92 start

Function

The **start** command sets the start mode and end mode for an NQA test instance.

The **undo start** command stops a running NQA test instance or restores the configuration of start mode and end mode of an unperformed NQA test instance.

By default, the test instance stops automatically after test packets are sent.

Format

start at [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]

start delay { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]

start now [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }]

undo start

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
start at [*yyyy/mm/dd*] *hh:mm:ss*	Performs a test instance at a specified time. **NOTE** The configured time must be later than the time on the device.	-
start delay { **seconds** *second* | *hh:mm:ss* }	Specifies a delay in performing a test instance.	• **seconds** *second*: specifies a delay in performing a test instance. The value is an integer ranging from 1 to 86399, in seconds. • *hh:mm:ss*: specifies a delay in performing a test instance. If *hh:mm:ss* is specified, the system automatically sets the moment in seconds. For example, 1:0:0 indicates that a test instance starts in one hour (3600 seconds).
start now	Performs a test instance immediately.	-
end at [*yyyy/mm/dd*] *hh:mm:ss*	Stops a test instance at a specified time.	-
end delay { **seconds** *second* | *hh:mm:ss* }	Specifies a delay in stopping a test instance. This delay is set based on the current system time. For example: If **start at 9:00:00 end delay seconds 60** is run at 8:59:40, then, a test instance starts at 9:00:00 and ends at 9:00:40.	• **seconds** *second*: specifies a delay in stopping a test instance. The value is an integer ranging from 6 to 86399 in seconds. • *hh:mm:ss*: specifies a delay in stopping a test instance. For example, 1:0:0 stands for a 3600-second delay from the current system time till the time that the test instance stops.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
end lifetime { **seconds** *second* | *hh:mm:ss* }	Specifies the lifetime of an NQA test instance (starting from the moment that the NQA test instance starts). For example: If **start delay seconds 60 end lifetime seconds 120** is run at 9:00:00, then, a test instance lasts for 120s as it starts at 09:01:00 and ends at 09:03:00.	• **seconds** *second*: sets the life time of a test instance in seconds. The value is an integer ranging from 6 to 86399 in seconds. • *hh:mm:ss*: sets the lifetime of a test instance. For example, 1:0:0 indicates that the lifetime of a test instance is 3600s starting from the moment a test instance starts.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After configuring test instances and relevant attributes, you need to manually set the start and end modes for the test instances. The types of start and end modes are as follows:

- Start modes:
  - Starting a test instance at a specified time
  - Starting a test instance immediately
  - Starting a test instance after a certain delay
- End modes:
  - Ending a test instance at a specified time
  - Ending a test instance immediately
  - Ending a test instance after a certain delay
  - Ending a test instance after all test packets are sent

You can set the start and end modes as required.

Precautions

If the number of the running test instances reaches the maximum value defined by the system, the **start** command is invalid.

For the same test instance, the **start now** command can be used again only when the previous configuration is complete.

When starting a test instance at a specified time, the time must be later than the current time on the device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Perform the test 10 hours later.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] destination-address ipv4 10.1.1.1
[Huawei-nqa-user-test] destination-port 4000
[Huawei-nqa-user-test] start delay 10:00:00
```

Related Topics

21.7.95 test-type

21.7.23 display nqa-agent

21.7.93 stop

Function

The **stop** command stops an NQA test instance.

Format

stop

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to stop only the running NQA test instances, that is, test instances in active state.

Example

Stop the test instance named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] stop
```

Related Topics

21.7.92 start

21.7.31 frequency

Copyright © Huawei Technologies Co., Ltd.

21.7.94 test-failtimes

Function

The **test-failtimes** command sets the number of consecutive test failures in an NQA test.

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

By default, a trap message is sent for each test failure.

Format

test-failtimes *times*

undo test-failtimes

Parameters

Parameter	Description	Value
times	Specifies the number of consecutive test failures in an NQA test.	The value is an integer that ranges from 1 to 15. The default value is 1.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An NQA test consists of multiple probe tests. By default, if one or more probe tests are successful in an NQA test, the test is considered successful. If all probe tests fail, the test is considered failed. If the number of consecutive test failures reaches the specified value, the system will send a trap to the specified NMS.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Follow-up Procedure

Run the **send-trap testfailure** command to send a trap to the NMS after an NQA test fails. Otherwise, the trap cannot be sent to the NMS after an NQA test fails.

Precautions

This configuration of a running test instance cannot be changed.

Copyright © Huawei Technologies Co., Ltd.

Example

Set the number of consecutive test failures to 10.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] test-failtimes 10
```

Related Topics

21.7.29 fail-percent

21.7.86 send-trap

21.7.95 test-type

Function

The **test-type** command configures the test type for an NQA test instance.

The **undo test-type** command cancels the test type configured for an NQA test instance.

By default, no test type is configured.

Format

test-type { **dhcp** | **dns** | **ftp** | **http** | **icmp** | **icmpjitter** | **jitter** | **lspping** | **lsptrace** | **snmp** | **tcp** | **trace** | **udp** | **vplsping** | **vplstrace** | **vplspwping** | **vplspwtrace** }

undo test-type

Parameters

Parameter	Description	Value
dhcp	Specifies a DHCP test.	-
dns	Specifies a DNS test.	-
ftp	Specifies an FTP service test.	-
http	Specifies an HTTP service test.	-
icmp	Specifies an ICMP test.	-
icmpjitter	Specifies an ICMP jitter test, which can detect the jitter on the network by using ICMP packets.	-
jitter	Specifies a jitter test, which can detect the jitter during UDP packet transmission.	-
lspping	Specifies an LSP ping test.	-
lsptrace	Specifies an LSP trace route test.	-
snmp	Specifies an SNMP test.	-
tcp	Specifies a TCP test.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
trace	Specifies a trace test.	-
udp	Specifies a UDP test.	-
vplsping	Specifies a VPLS MAC ping test.	-
vplstrace	Specifies a VPLS MAC trace test.	-
vplspwping	Specifies a VPLS PW ping test.	-
vplspwtrace	Specifies a VPLS PW trace test.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The type of a running test instance cannot be changed.

Example

Configure the test type of an NQA test instance as TCP.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type tcp
```

Related Topics

21.7.56 nqa

21.7.96 timestamp-unit

Function

The **timestamp-unit** command sets the unit of timestamp for an NQA test instance.

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

By default, the unit of timestamp for an NQA test instance is millisecond.

Format

timestamp-unit { **millisecond** | **microsecond** }

undo timestamp-unit microsecond

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
millisecond	Sets the unit of timestamp for an NQA test instance to millisecond.	-
microsecond	Sets the unit of timestamp for an NQA test instance to microsecond.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **timestamp-unit millisecond** command sets the unit of timestamp for an NQA test instance to millisecond.

The **timestamp-unit microsecond** command sets the unit of timestamp for an NQA test instance to microsecond.

Prerequisites

Hardware forwarding has been enabled using the **hardware-based enable** command.

Precautions

The **timestamp-unit** command takes effect for only jitter test instances.

Example

Set the unit of timestamp for an NQA test instance to microsecond.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] hardware-based enable
[Huawei-nqa-user-test] timestamp-unit microsecond
```

Related Topics

21.7.56 nqa

21.7.97 threshold

Function

The **threshold** command sets the OWD and RTD threshold.

The **undo threshold** command deletes the OWD threshold and the RTD threshold.

Copyright © Huawei Technologies Co., Ltd.

By default, no threshold is set.

Format

threshold { **owd-ds** *owd-ds-value* | **owd-sd** *owd-sd-value* | **rtd** *rtd-value* }

undo threshold { **owd-ds** | **owd-sd** | **rtd** }

Parameters

Parameter	Description	Value
owd-ds *owd-ds-value*	Sets the OWD threshold of packets sent from the destination to the source.	The value is an integer that ranges from 1 to 60000. The unit of this value is the same as that of the timestamp set using the **timestamp-unit** command.
owd-sd *owd-sd-value*	Sets the OWD threshold of packets sent from the source to the destination.	The value is an integer that ranges from 1 to 60000. The unit of this value is the same as that of the timestamp set using the **timestamp-unit** command.
rtd *rtd-value*	Sets the RTD threshold.	The value is an integer that ranges from 1 to 60000. The unit of this value is the same as that of the timestamp set using the **timestamp-unit** command.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The OWD threshold is applied only to jitter test instances.

Example

Set the RTD threshold to 2 ms.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] threshold rtd 2
```

Related Topics

21.7.86 send-trap

Copyright © Huawei Technologies Co., Ltd.

21.7.98 timeout

Function

The **timeout** command sets the timeout period for a probe of an NQA test instance.

The **undo timeout** command restores the default timeout period for a probe of an NQA test instance.

By default, the timeout period for DHCP and FTP test instances is 15 seconds and that for other test instances is 3 seconds.

Format

timeout *time*

undo timeout

Parameters

Parameter	Description	Value
time	Specifies the timeout period for a probe.	The value is an integer that ranges from 1 to 60, in seconds.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The timeout period refers to the waiting time after a probe is sent. If no response packet is received when the timeout period expires, the probe fails. The timeout period is set based on the actual networking. If the value is too small, the NQA test instance fails.

On an unstable network with a low transmission rate, you need to prolong the timeout period for sending probe packets to ensure that response packets can be received.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Precautions

- You are advised to set the timeout period based on the round-trip time (RTT) value. Ensure that the timeout period set by the **timeout** command is longer than the RTT value.

Copyright © Huawei Technologies Co., Ltd.

- In all test instances except jitter test instance, the timeout period set by the **timeout** command must be smaller than or equal to the interval of automatic tests set by the **interval** command. Otherwise, the tests fail due to timeout of test packets.
- In a DHCP test, packets are sent at random within 10 seconds. If the timeout period is shorter than 10 seconds, some or all packets may time out. Therefore, in a DHCP test, the timeout period must be longer than 10 seconds. The default timeout period is 15 seconds.

Precautions

You cannot change this configuration of a running test instance.

In an ICMP test instance, if the following conditions are met, the Completion field in the test results will be displayed as **no result**:

- The system CPU usage exceeds 90% and the configured timeout period is less than 6s.
- **frequency** configured ≤ (**probe-count** - 1) × **interval** + 6.

Example

Set the timeout period of the test instance named **user test** to 20 seconds.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] timeout 20
```

Related Topics

21.7.31 frequency

21.7.41 interval (NQA view)

21.7.99 tos

Function

The **tos** command sets the ToS value for an NQA test packet.

The **undo tos** command restores the default ToS value of an NQA test packet.

By default, the ToS value is 0.

Format

tos *value*

undo tos

Parameters

Parameter	Description	Value
value	Specifies the ToS value of a packet.	The value is an integer that ranges from 0 to 255. The default value is 0.

Copyright © Huawei Technologies Co., Ltd.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The ToS field contains a precedence sub-field and a ToS sub-field. The precedence sub-field indicates the priority of a packet and the ToS sub-field is seldom used. All the bits in the ToS sub-field must be set to 0. You can set the priority of probe packets by setting the ToS value. When a large number of packets are received, packets of high priorities are processed preferentially.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The following types of test instances are not supported:

- DNS
- DHCP
- Trace
- LSP Ping
- LSP Trace

Configuration Impact

If you run the **tos** command multiple times, only the latest configuration takes effect.

Precautions

The ToS value of a running test instance cannot be changed.

Example

Set the ToS value for the test instance named **user test** to 10.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] tos 10
```

Related Topics

21.7.95 test-type

21.7.56 nqa

Copyright © Huawei Technologies Co., Ltd.

21.7.100 tracert-hopfailtimes

Function

The **tracert-hopfailtimes** command sets the number of consecutive failed hops indicating a failed trace test instance.

The **undo tracert-hopfailtimes** command restores the default number of consecutive failed hops indicating a failed trace test instance.

By default, five consecutive failed hops indicates a failed trace test instance.

Format

tracert-hopfailtimes *times*

undo tracert-hopfailtimes

Parameters

Parameter	Description	Value
times	Specifies the number of consecutive failed hops indicating a failed trace test instance.	The value is an integer that ranges from 1 to 255.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **tracert-hopfailtimes** command only takes effect for trace and LSP trace test instances.

You cannot change this configuration of a running test instance.

Example

Set the number of consecutive failed hops indicating a failed trace test instance to 6.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type trace
[Huawei-nqa-user-test] tracert-hopfailtimes 6
```

Related Topics

21.7.95 test-type

Copyright © Huawei Technologies Co., Ltd.

21.7.101 tracert-livetime

Function

The **tracert-livetime** command sets the time to live (TTL) value for trace test instances in an NQA test.

The **undo tracert-livetime** command restores the default TTL value for trace test instances in an NQA test.

By default, the initial TTL value is 1 and the maximum TTL value is 30.

Format

tracert-livetime first-ttl *first-ttl* **max-ttl** *max-ttl*

undo tracert-livetime

Parameters

Parameter	Description	Value
first-ttl *first-ttl*	Specifies the initial TTL value of a packet.	The value is an integer that ranges from 1 to 255. The default value is 1.
max-ttl *max-ttl*	Specifies the maximum TTL value of a packet.	The value is an integer that ranges from 1 to 255. The value of *max-ttl* must be greater than the value of *first-ttl*. By default, the maximum TTL value is 30.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **tracert-livetime** command takes effect only for trace and LSP trace test instances.

You cannot change this configuration of a running test instance.

Example

Set the initial TTL value of the test instance named **user test** to 5 and the maximum TTL value to 20.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type trace
[Huawei-nqa-user-test] tracert-livetime first-ttl 5 max-ttl 20
```


Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.95 test-type

21.7.102 ttl

Function

The **ttl** command sets the TTL value for the test packets of an NQA test instance.

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

The default TTL value is 30.

Format

ttl *number*

undo ttl

Parameters

Parameter	Description	Value
number	Specifies the TTL value.	The value is an integer that ranges from 1 to 255. The default TTL value is 30.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent test packets from being transmitted endlessly, the test instance must be performed within certain hops.

When a test packet is created, you can run the **ttl** command to set the TTL value. When the test packet is transmitted along Layer 3 routing devices, each Layer 3 routing device decrements the TTL value by one when the packet arrives. When the TTL value is 0, the Layer 3 routing device discards the test packet and sends an error message to the sending end. This prevents test packets from being transmitted endlessly.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The type of test instances that are not supported is as follows:

- DNS

Copyright © Huawei Technologies Co., Ltd.

- DHCP
- Trace
- LSP Trace

Configuration Impact

If you run the **ttl** command multiple times, only the latest configuration takes effect.

Precautions

The type of a running test instance cannot be changed.

Example

Set the TTL value for the test packets of a test instance named **user test** to 10.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] ttl 10
```

Related Topics

21.7.95 test-type

21.7.103 ttl-copymode

Function

Using the **ttl-copymode** command, you can specify the TTL propagation mode (pipe or uniform) for a multi-hop PW detection.

Using the **undo ttl-copymode** command, you can cancel the TTL propagation mode configured in the NQA view.

By default, the TTL propagation mode varies with products.

Format

ttl-copymode { **pipe** | **uniform** }

undo ttl-copymode

Parameters

Parameter	Description	Value
pipe	Sets the TTL propagation mode to pipe.	-
uniform	Sets the TTL propagation mode to uniform.	-

Views

NQA view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

During the detection of a multi-hop PW, if the default TTL propagation mode on different devices is different, you need to specify the TTL propagation mode on the first hop of the PW. This command is used to detect BGP/MPLS IP VPN networks.

The TTL propagated in pipe and uniform modes is processed in different manners:

- When receiving a packet carrying the TTL propagated in pipe mode, the system strips the outer tag of the packet, decreases the TTL in the inner tag by 1, and then sets the TTL in the outer tag to 255.
- When receiving a packet carrying the TTL propagated in uniform mode, the system maps the TTL in the outer tag to the inner tag, decreases the TTL in the inner tag by 1, and then sets the TTL in the outer tag to the value of the TTL in the inner tag.

NOTE

The **ttl-copymode** command makes sense only in the trace test instances. In the case of an trace test instance, you need to first run the **vpn-instance** *vpn-instance-name* command to bind the NQA trace test instance with a VPN instance.

Example

Configure the TTL propagation mode of packets in the NQA trace test instance as pipe.

```
<Huawei> system-view
[Huawei] nqa test-instance admin trace
[Huawei-nqa-admin-trace] test-type trace
[Huawei-nqa-admin-trace] vpn-instance voice
[Huawei-nqa-admin-trace] ttl-copymode pipe
```

Related Topics

21.7.95 test-type

21.7.104 vlan (NQA view)

Function

Using the **vlan** command, you can configure a VLAN ID for the NQA test instance.

Using the **undo vlan** command, you can delete a specified VLAN.

By default, no VLAN ID is configured.

Format

vlan *vlan-id*

undo vlan

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlan *vlan-id*	Indicates a VLAN. *vlan-id* specifies the VLAN ID.	*vlan-id* is an integer that ranges from 1 to 4094.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

If both the destination MAC address and the specified VLAN need to be matched, you need to set a VLAN ID.

The test instances that can be configured with a VLAN ID include:

- vplsping
- vplstrace
- vplspwping
- vplspwtrace
- vplsmping
- vplsmtrace
- gmacping
- gmactrace
- generalflow

Example

Set the VLAN ID of the test instance to 1.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type vplsping
[Huawei-nqa-user-test] vlan 1
```

Related Topics

6.3.43 vlan

21.7.105 vpn-instance

Function

The **vpn-instance** command configures the VPN instance that an NQA test instance belongs to.

The **undo vpn-instance** command deletes the configured VPN instance.

Copyright © Huawei Technologies Co., Ltd.

By default, no VPN instance is configured.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the VPN instance that an NQA test instance belongs to.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **vpn-instance** command does not take effect for DNS, LSP ping, LSP trace, and DHCP test instances.

Example

Set the VPN instance for an NQA test instance named **user test** to vrf1.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] vpn-instance vrf1
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.8 LSDP Configuration Commands

NOTE

An AR3200 has active/standby MPUs installed. An active/standby switchover between the MPUs will also cause the interface status to alternate between Down and Up. It is difficult to determine whether the interface status change is caused by MPU switchover or LSDP. Therefore, you are not advised to configure LSDP on an AR3200.

Copyright © Huawei Technologies Co., Ltd.

21.8.1 lsdp

Function

The **lsdp** command configures LSDP on a device.

The **undo lsdp** command disables LSDP on a device.

By default, the LSDP function is disabled on a device.

Format

lsdp *ip-address* [*nexthop-address*] [**interval** *interval-number*] [**probe-count** *count-number*]

undo lsdp

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address of probe packets.	The value is in dotted decimal notation.
nexthop-address	Specifies the next-hop IP address of probe packets.	The value is in dotted decimal notation.
interval *interval-number*	Specifies the interval for sending probe packets.	The value is an integer that ranges from 100 to 10000, in milliseconds. The default value is 1000. That is, the device sends a probe packet every second.
probe-count *count-number*	Specifies the maximum number of probe counts upon probe failures.	The value is an integer that ranges from 3 to 10. The default value is 3. That is, the device considers a probe failed if the device does not receive a reply packet after three ARP or ICMP request packets are sent. Then the device sets the interface status to Down.

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After the **lsdp** command is executed on an interface, the interface sends probe packets (ARP and ICMP packets) to the destination address to detect link connectivity. If the interface receives a reply packet within a probe interval, LSDP considers the destination address reachable. In this situation, the probe is successful and LSDP sets the interface status to Up. If the interface does not receive a reply packet within a probe interval, LSDP considers the destination address unreachable. In this situation, the probe fails, LSDP sets the interface status to Down, and services on this interface become invalid.

The probe intervals are calculated as follows:

- Interval for sending ARP packets: *interval-number***count-number*
- Interval for sending ICMP packets: *interval-number**(*count-number*+n)

  n is the number of sent ARP packets. The value ranges from 1 to *count-number*.

The default value of *interval-number* is 1000. That is, the device sends a probe packet every second. The default value of *count-number* is 3. That is, an LSDP probe fails if the interface does not receive an ARP reply packet within 3x1 seconds or an ICMP reply packet within (3+n)x1 seconds. Then LSDP sets the interface status to Down. When the default value of *count-number* is used, n can be 1, 2, or 3, indicating that the interface receives an ARP reply packet after sending 1, 2, or 3 ARP request packets.

After LSDP sets the status of an interface to Down, the device continuously sends ARP and ICMP packets for probing. When the link is recovered, LSDP sets the interface to Up.

Configuration Impact

The interface with LSDP configured periodically sends ARP and ICMP packets. When LSDP detects that the link to a destination address fails, it sets the interface status to Down.

Example

Configure an interface to send one LSDP probe packet to destination address 10.1.1.1 through next-hop address 10.10.1.1 every 100 milliseconds and set the maximum number of probe counts to 5.

```
<Huawei> system-view
[Huawei] interface gigabitethernet1/0/0
[Huawei-GigabitEthernet1/0/0] lsdp 10.1.1.1 10.10.1.1 interval 100 probe-count 5
```

Related Topics

21.8.3 display lsdp

 Copyright © Huawei Technologies Co., Ltd.

21.8.2 lsdp trigger protocol ospf delay-up

Function

The **lsdp trigger protocol ospf delay-up** command configures a delay in sending OSPF packets after LSDP detects that a link goes Up.

The **undo lsdp trigger protocol** command restores the default configuration.

By default, no delay is configured for the device to send OSPF packets after LSDP detects that a link goes Up.

Format

lsdp trigger protocol ospf delay-up *delay-time*

undo lsdp trigger protocol

Parameters

Parameter	Description	Value
delay-time	Specifies a delay.	The value is an integer that ranges from 1 to 3600, in seconds.

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When LSDP detects that a link goes Down, OSPF packets will be blocked. You can run the **lsdp trigger protocol ospf delay-up** command to configure a delay in sending OSPF packets after LSDP detects that a link goes Up.

Prerequisites

The destination IP address to which probe packets are sent has been configured using the **lsdp** command.

Example

Set the delay in sending OSPF packets after LSDP detects that the link goes Up to 10 seconds.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] lsdp trigger protocol ospf delay-up 10
```

21.8.3 display lsdp

Function

The **display lsdp** command displays the LSDP information.

Format

display lsdp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view LSDP configuration, running status, and running results.

Example

View the LSDP information.

```
<Huawei> display lsdp
======LSDP INFO=========
LSDP Instance Index : 1
LSDP Test : success
LSDP Interface Name : GigabitEthernet0/0/0
LSDP Interface Status : UP
LSDP Interface Ip : 10.1.2.1
LSDP Destination Ip : 10.1.4.2
LSDP Next-hop Ip : 10.1.2.2
LSDP Interval : 1000
LSDP Probe-count : 3
LSDP UpTimes : 0
LSDP DownTimes : 0
========================
```

Table 21-60 Description of the **display lsdp** command output

Item	Description
LSDP Instance Index	LSDP table index.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
LSDP Test	Current LSDP probe result. • success: Probe is successful. • fail: Probe fails. • --: No result.
LSDP Interface Name	Types and numbers of the interface where LSDP is configured.
LSDP Interface Status	Status of the interface where LSDP is configured.
LSDP Interface Ip	IP address of the interface where LSDP is configured.
LSDP Destination Ip	Destination IP address of probe packets. To configure the destination IP address of probe packets, run the **lsdp** command.
LSDP Next-hop Ip	Next-hop IP address of probe packets. To configure the next-hop IP address of probe packets, run the **lsdp** command.
LSDP Interval	Interval for sending probe packets. To configure the interval for sending probe packets, run the **lsdp** command.
LSDP Probe-count	Maximum number of probe counts upon probe failures. To configure the maximum number of probe counts, run the **lsdp** command.
LSDP UpTimes	Maximum number of times an interface goes Up after LSDP is configured.
LSDP DownTimes	Maximum number of times an interface goes Down after LSDP is configured.

Related Topics

21.8.1 lsdp

21.9 Service Diagnosis Configuration Commands

21.9.1 display trace information

Copyright © Huawei Technologies Co., Ltd.

Function

The **display trace information** command displays information about service diagnosis.

Format

display trace information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring service diagnosis, you can run this command to view global information about service diagnosis, for example, the counts of diagnosis instances and objects created on the device.

Example

Display information about service diagnosis.

```
<Huawei> display trace information
Trace Information:
-------------------------------------------------------------
Trace Enable                      : Enable
Debug info level                  : Brief
Debug fill-instance               : Off
Debug quit-instance               : Off
Debug output information          : Off
Syslog Source IP Address          : -

The sum of all the instances      : 0
The startID of the instance table  : -
Alloc instance times              : 9
Free instance times               : 9
The sum of all the objects        : 2
-------------------------------------------------------------
```

Table 21-61 Description of the display trace information command output

Item	Description
Trace Information	Information about service diagnosis.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trace Enable	Status of service diagnosis. • Disable: Service diagnosis is disabled. • Enable: Service diagnosis is enabled. This field can be modified using the **trace enable** command.
Debug info level	Output level of service diagnosis information. • Brief: brief service diagnosis information. • Detail: detailed service diagnosis information. This field can be modified using the **trace enable** command.
Debug fill-instance	Debugging status of the **fill-instance** module. • Off: disabled • On: enabled
Debug quit-instance	Debugging status of the **quit-instance** module. • Off: disabled • On: enabled
Debug output information	Debugging status of the **output information** module. • Off: disabled • On: enabled
Syslog Source IP Address	IP address of the interface for exporting diagnosis information to the log server. To set the IP address of the interface for exporting diagnosis information to a log server, run the **trace syslog source** command.
The sum of all the instances	Total number of diagnosis instances.
The startID of the instance table	Start ID of the instance table.
Alloc instance times	Number of the allocated diagnosis instances.
Free instance times	Number of the release diagnosis instances.
The sum of all the objects	Total number of diagnosis objects.

Related Topics

21.9.6 trace enable

21.9.8 trace syslog source

 Copyright © Huawei Technologies Co., Ltd.

21.9.2 display trace instance

Function

The **display trace instance** command displays diagnosis instances on a device.

Format

display trace instance [*instance-start-id* [*instance-end-id*] | **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* | **cid** *cid*] [**slot** *slot-id*]

Parameters

Parameter	Description	Value
instance-start-id	Specifies the ID of the first instance whose information is displayed, that is, start ID.	The value varies according to different devices.
instance-end-id	Specifies the ID of the last instance whose information is displayed, that is, end ID.	The value varies according to different devices. **NOTE** The *instance-end-id* value must be larger than the *instance-start-id* value.
mac-address *mac-address*	Specifies a MAC address.	The value is in the format of H-H-H, in which H is a hexadecimal number of 4 digits.
ip-address *ip-address*	Specifies an IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters without spaces.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
cid *cid*	Specifies the diagnosis instance CID.	The value varies according to different devices.
slot *slot-id*	Specifies the slot ID of an interface card.	The value varies according to different devices.

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you specify no parameter, all diagnosis instances are displayed in sequence. Each time you run this command, 10 diagnosis instances are displayed. For example, all diagnosis instances have been created on the device. When you run the **display trace instance** command for the first time, information about diagnosis instances 0 to 9 is displayed. When you run this command again, information about instances 10 to 19 is displayed. This process is repeated until information about all the diagnosis instances is displayed. If you specify the value of *instance-start-id*, information about 10 diagnosis instances from this ID is displayed.

To view information about diagnosis instances within a specified range, run the **display trace instance** *instance-start-id instance-end-id* command to specify the start and end IDs of diagnosis instances.

Example

Display information about diagnosis instances on the interface with the IP address of 10.10.10.1.

```
<Huawei> display trace instance ip-address 10.10.10.1
Trace Instance:
------------------------------------------------------------------
 ID            : 0
 MAC Address    : 00e0-fc03-0203
 IP Flag        : -
 Session ID     : 4
 IP Address     : 10.10.10.1
 VRF Index      : -
 CID            : -
 Calling Number : -
 SubCallingNum  : NO
 User Name      : -
 Interface      : -
 QinQ VLAN ID   : -
 User VLAN ID   : -
 Access Mode    : pppoe
 User Tunnel ID : -
 Modules online : EAPoL  :0    WEBS   :0    WEB    :0    AAA    :0
                  CM     :0    TM     :0    SAM    :0    RADIUS :0
                  DHCPS  :0    DHCPC  :0    DHCPR  :0    DHCPP  :0
                  TACACS :0    AM     :0    SAVI   :0    WLAN_AC:0
                  L2TP   :0    LNS    :0    PPP    :0    PPPOE  :1
                  PPPOLNS:0
------------------------------------------------------------------
 Total 1, 1 printed
```

Table 21-62 Description of the display trace instance command output

Item	Description
ID	ID of the diagnosis instance.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
MAC Address	MAC address of the interface.
IP Flag	Flag of the IP address.
Session ID	ID of the session, only valid for PPPoX users.
IP Address	IP address of the interface.
VRF Index	User VRF index.
CID	User connect ID.
Calling Number	User calling number.
SubCallingNum	Whether fuzzy matching is supported.
User Name	User name.
Interface	Interface index.
QinQ VLAN ID	QinQ VLAN ID.
User VLAN ID	User VLAN ID.
Access Mode	User access mode.
User Tunnel ID	User tunnel ID.
Modules online	User status on a module. User status can be: • 0: The user is offline on the module. • 1: The user is online on the module.

Related Topics

21.9.7 trace object

21.9.3 display trace object

Function

The **display trace object** command displays the configuration about a service diagnosis object.

Format

display trace object [*service-object-id*] [**slot** *slot-id*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
service-object-id	Specifies the ID of a diagnosis object.	The value is an integer that ranges from 0 to 3.
slot *slot-id*	Specifies the slot ID of an interface card.	The value varies according to different devices.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you do not specify the parameters *service-object-id* and **slot**, configurations about all diagnosis objects are displayed.

Example

Display configurations about all diagnosis objects.

```
<Huawei> display trace object
Trace Object:
------------------------------------------------------------
  Object ID      : 0
  Slot           : -
  MAC Address    : -
  IP Flag        : -
  Session ID     : -
  IP Address     : 1.1.1.1
  VRF Index      : -
  CID            : -
  Calling Number : -
  SubCallingNum  : NO
  User Name      : -
  Interface      : -
  QinQ VLAN ID   : -
  User VLAN ID   : -
  Access Mode    : -
  User Tunnel ID : -
  Output         : command line ( User-Intf 131 )

  Object ID      : 1
  Slot           : -
  MAC Address    : -
  IP Flag        : -
  Session ID     : -
  IP Address     : -
  VRF Index      : -
  CID            : -
  Calling Number : -
  SubCallingNum  : NO
  User Name      : huawei
  Interface      : -
```


Copyright © Huawei Technologies Co., Ltd.

```
QinQ VLAN ID   : -
User VLAN ID   : -
Access Mode    : -
User Tunnel ID : -
Output         : command line ( User-Intf 131 )

Object ID      : 2
Slot           : -
MAC Address    : 0101-0101-0101
IP Flag        : -
Session ID     : -
IP Address     : -
VRF Index      : -
CID            : -
Calling Number : -
SubCallingNum  : NO
User Name      : -
Interface      : -
QinQ VLAN ID   : -
User VLAN ID   : -
Access Mode    : -
User Tunnel ID : -
Output         : command line ( User-Intf 131 )

------------------------------------------------------------------
Total 3, 3 printed
```

Table 21-63 Description of the display trace object command output

Item	Description
Object ID	ID of the diagnosis object. This parameter is automatically generated from 0 in sequence of creation time.
Slot	Slot ID of the interface board.
MAC Address	MAC address of the interface. To set the MAC address of an interface, run the **trace object** command.
IP Flag	Flag of the IP address.
Session ID	ID of the session, only valid for PPPoX users.
IP Address	IP address of the interface. To set the IP address of an interface, run the **trace object** command.
VRF Index	User VRF index.
CID	User connect ID.
Calling Number	User calling number. To set the calling number, run the **trace object** command.
SubCallingNum	Whether fuzzy matching is supported. To set the SubCallingNum, run the **trace object** command.
User Name	User name. To set the user name, run the **trace object** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Interface	Interface index. To set the interface index, run the **trace object** command.
QinQ VLAN ID	QinQ VLAN ID. To set the QinQ VLAN ID, run the **trace object** command.
User VLAN ID	User VLAN ID. To set the user VLAN ID, run the **trace object** command.
Access Mode	User access mode, including dot1x, mac-authen, portal, wlan, pppoe, and pppolns. To set the user access mode, run the **trace object** command.
User Tunnel ID	User tunnel ID. To set the user tunnel ID, run the **trace object** command.
Output	Direction in which the device exports diagnosis information. To set the direction, run the **trace object** command. • Command line (User-Intf X): Diagnosis information is displayed on the screen of a configuration terminal. **NOTE** When the configuration terminal is online, X displays the absolute number of the user interface (the absolute number can be checked using the **display users** command). When the configuration terminal is offline, X displays offline. • file: Diagnosis information is exported to files. • server: Diagnosis information is exported to a log server.
Total 3, 3 printed	Total number of created diagnosis objects and count of displayed objects.

Related Topics

21.9.7 trace object

21.9.4 reset trace instance

Function

The **reset trace instance** command clears all the diagnosis instances on a device.

Format

reset trace instance

Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After service diagnosis is enabled and a diagnosis object is created on a device, the device creates a diagnosis instance when a user matching the attributes of the diagnosis object gets online. If the device diagnoses services of multiple users, it creates a diagnosis instance for each user, which occupies a large amount of system resources. Therefore, the device needs to delete the diagnosis instance of a user when the user goes online successfully or fails to go online. Additionally, the device provides an aging mechanism for service diagnosis. When the aging time is reached, the device automatically deletes diagnosis instances to reclaim resources.

In addition to the preceding two methods for automatically clearing diagnosis instances, you can run the **reset trace instance** command to clear all the diagnosis instances.

NOTICE

After all the diagnosis instances are cleared using the **reset trace instance** command, properly running diagnosis instances are also deleted. Exercise caution when you run the **reset trace instance** command.

Example

Clear all diagnosis instances on the device.

```
<Huawei> system-view
[Huawei] reset trace instance
```

Related Topics

21.9.2 display trace instance

21.9.5 save trace information

Function

The **save trace information** command saves diagnosis information in the buffer area as a file.

Copyright © Huawei Technologies Co., Ltd.

Format

save trace information

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

After you specify the parameter **file** *file-name* in the **trace object** command to save diagnosis information as files to the default root directory on the storage device, the system saves diagnosis information in the buffer area until the buffer is full. To prevent data loss, the system automatically saves diagnosis information in the buffer area as the file *file-name*. Before the buffer becomes full, to view real-time diagnosis information, run the **save trace information** command to save diagnosis information in the buffer area as a file.

Prerequisites

The device has been configured to export diagnosis information as a file using the **trace object** command.

Example

Save diagnosis information as a file.

```
<Huawei> system-view
[Huawei] save trace information
```

Related Topics

21.9.7 trace object

21.9.6 trace enable

Function

The **trace enable** command enables service diagnosis.

The **undo trace enable** command disables service diagnosis.

By default, service diagnosis is disabled.

Copyright © Huawei Technologies Co., Ltd.

Format

trace enable [**brief**]

undo trace enable

Parameters

Parameter	Description	Value
brief	Configures the device to output brief service diagnosis information.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

It is difficult to locate problems during user access based on debugging information on existing networks because multiple users may get online or offline simultaneously and debugging information about a specified user cannot be displayed. Service diagnosis provided by the router allows maintenance personnel to customize attributes and create diagnosis objects to diagnose information about services of specified users. To enable service diagnosis, run the **trace enable** command.

Service diagnosis information can be displayed in two methods:

- The **trace enable brief** command configures the device to output brief service diagnosis information.
- The **trace enable** command configures the device to output detailed service diagnosis information.

Follow-up Procedure

After service diagnosis is enabled, run the **trace object** command to create a diagnosis object. After an ID is generated for the diagnosis object, the system starts diagnosis services.

Precautions

Service diagnosis affects system performance. Therefore, enable service diagnosis only when fault locating is required. After locating faults, immediately run the **undo trace enable** command to disable service diagnosis.

Copyright © Huawei Technologies Co., Ltd.

The **trace enable** command is not recorded in the configuration file. Therefore, run the **trace enable** command again after the device restarts to make service diagnosis take effect.

Example

Enable the service diagnosis function and configure the device to output brief service diagnosis information.

```
<Huawei> system-view
[Huawei] trace enable brief
```

Related Topics

21.9.7 trace object

21.9.7 trace object

Function

The **trace object** command creates a diagnosis object.

The **undo trace object** command deletes a diagnosis object.

By default, no diagnosis object is created. If you do not specify the direction at which information is exported, the default direction is the CLI.

Format

trace object { **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* | **user-vlan** *user-vlan-id* [**qinq-vlan** *qinq-vlan-id*] | **user-name** *user-name* | **access-mode** { **dot1x** | **mac-authen** | **portal** | **wlan** | **pppoe** | **pppolns** } } * [**slot** *slot-id*] [**output** { **command-line** | **file** *file-name* | **syslog-server** *syslog-server-ip* }]

trace object calling-number [**output** { **command-line** | **file** *file-name* | **syslog-server** *syslog-server-ip* }] [**slot** *slot-id*] [| **include**] **calling-number-content** *text*

trace object tunnel-id *tunnel-id* [**slot** *slot-id*] [**output** { **command-line** | **file** *file-name* | **syslog-server** *syslog-server-ip* }]

undo trace object { **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* | **user-vlan** *user-vlan-id* [**qinq-vlan** *qinq-vlan-id*] | **user-name** *user-name* | **access-mode** { **dot1x** | **mac-authen** | **portal** | **wlan** | **pppoe** | **pppolns** } } * [**slot** *slot-id*] [**output** { **command-line** | **file** *file-name* | **syslog-server** *syslog-server-ip* }]

undo trace object { *service-object-id* | **all** }

undo trace object { **calling-number** [| **include**] **calling-number-content** *text* | **tunnel-id** *tunnel-id* }

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mac-address *mac-address*	Creates a diagnosis object based on the MAC address.	The value is in the format of H-H-H, in which H is a hexadecimal number of 4 digits.
ip-address *ip-address*	Creates a diagnosis object based on the IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters without spaces.
interface *interface-type interface-number*	Creates a diagnosis object based on the interface.	-
user-vlan *user-vlan-id*	Creates a diagnosis object based on the user VLAN.	The value is an integer that ranges from 1 to 4094.
qinq-vlan *qinq-vlan-id*	Creates a diagnosis object based on the QinQ VLAN ID.	The value is an integer that ranges from 1 to 4094.
user-name *user-name*	Creates a diagnosis object based on the user name.	The value is a string of 1 to 253 case-insensitive characters without spaces.
access-mode	Creates a diagnosis object based on the access mode.	-
dot1x	Creates a diagnosis object based on the dot1x access mode.	-
mac-authen	Creates a diagnosis object based on the mac-authen access mode.	-
portal	Creates a diagnosis object based on the portal access mode.	-
wlan	Creates a diagnosis object based on the wlan access mode.	-
pppoe	Creates a diagnosis object based on the pppoe access mode.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pppolns	Creates a diagnosis object based on the pppolns access mode.	-
| **include**	Whether fuzzy matching is supported.	-
calling-number-content *text*	Creates a diagnosis object based on the calling number.	The value varies according to different devices.
tunnel-id *tunnel-id*	Creates a diagnosis object based on the tunnel ID.	The value varies according to different devices.
slot *slot-id*	Specifies the slot ID of an interface card.	The value varies according to different devices.
output	Specifies the direction in which the device exports diagnosis information.	-
command-line	Exports diagnosis information to the CLI.	-
file *file-name*	Exports diagnosis information as a file. **NOTE** It is recommended that you export the diagnosis information to a specified file.	The value of *file-name* is a string of 1 to 63 case-insensitive characters without spaces.
syslog-server *syslog-server-ip*	Exports diagnosis information to a log server.	*syslog-server-ip* specifies the IP address of the log server, in dotted decimal notation.
service-object-id	Specifies the ID of a diagnosis object to be deleted. **NOTE** Diagnosis object IDs are generated based on sequence in which the diagnosis objects are created. The ID starts from 0. To view all created diagnosis objects, run the **display trace object** command.	The value is an integer that ranges from 0 to 3.
all	Deletes all diagnosis objects.	-

Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

When locating faults of DHCP, L2TP, AAA, or NAC service during user access, maintenance personnel can create diagnosis objects to trace services and locate the faults.

Users with different services have different attributes. Create diagnosis objects for different services based on different attributes.

- DHCP service: based on the MAC address.
- L2TP service: based on the calling number and tunnel ID.
- AAA and NAC services: based on the MAC address, IP address, user name, user VLAN ID, access mode, or interface number.

NOTE

To ensure that you can diagnose the entire DHCP service process, create a diagnosis object based on the MAC address. You can run the **trace object mac-address** *mac-address* [**output** { **command-line** | **file** *file-name* | **syslog-server** *syslog-server-ip* }] command to create a diagnosis object for the DHCP service.

Service diagnosis supports only common AAA users.

Prerequisites

Service diagnosis has been enabled using the **trace enable** command.

Precautions

The diagnosis output file cannot exceeds 1 MB. The excessive diagnosis information is not recorded.

You can run the **undo trace object** command to delete diagnosis objects in any of the following modes:

- Delete diagnosis objects based on the object attributes. Run the **undo trace object** { **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* | **user-vlan** *user-vlan-id* [**qinq-vlan** *qinq-vlan-id*] | **user-name** *user-name* | **access-mode** { **dot1x** | **mac-authen** | **portal** | **wlan** | **pppoe** | **pppolns** } } * or **undo trace object** { **calling-number** [| **include**] **calling-number-content** *text* | **tunnel-id** *tunnel-id* } command. For example, diagnosis objects 1 (10.10.10.1) and 2 (10.10.10.1+0025-9efb-be78) have been created. To delete diagnosis objects based on the IP address, run the **undo trace object ip-address 10.10.10.1** command. Diagnosis objects 1 and 2 are deleted.
- Delete diagnosis objects based on the object ID. Run the **undo trace object** *service-object-id* command to delete a specified diagnosis object. You can view the object ID using the **display trace object** command

Copyright © Huawei Technologies Co., Ltd.

- Delete all diagnosis objects using the **undo trace object all** command.

Example

Create a diagnosis instance on the interface with the IP address of 10.10.10.1.

```
<Huawei> system-view
[Huawei] trace object ip-address 10.10.10.1
```

Related Topics

21.9.3 display trace object
21.9.6 trace enable

21.9.8 trace syslog source

Function

The **trace syslog source** command sets the source interface from which the device exports diagnosis information to a log server.

The **undo trace syslog source** command cancels the configuration of the source interface from which the device exports diagnosis information to a log server.

By default, no interface is specified to export diagnosis information to the log server.

Format

trace syslog source *interface-type interface-number*

undo trace syslog source

Parameters

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

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

After you specify an interface for exporting diagnosis information to a log server, the system specifies the IP address of this interface as the source IP address of

Copyright © Huawei Technologies Co., Ltd.

service diagnosis packets. In this way, the log server can identify the source of diagnosis information.

Prerequisites

The device has been configured to export diagnosis information to a log server using the **trace object** command.

Precautions

The **trace syslog source** command is not recorded in the configuration file. After the device restarts, the configured source interface for exporting diagnosis information is invalid. To set the source interface, run the **trace syslog source** command again.

Example

Set GE1/0/0 as the source interface for exporting diagnosis information to the log server.

```
<Huawei> system-view
[Huawei] trace syslog source gigabitethernet 1/0/0
```

Related Topics

21.9.7 trace object

21.10 Mirroring Configuration Commands

NOTE

The device supports mirroring. The mirroring function is used for network detection and fault management, and may involve personal communication information. Huawei cannot collect or store user communication information without permission. It is recommended that relevant functions used to collect or store user communication information be enabled under applicable laws and regulations. During user communication information usage and storage, measures must be taken to protect user communication information.

21.10.1 display mirror-port

Function

The **display mirror-port** command displays the port mirroring configuration.

Format

display mirror-port

Parameters

None

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

None

Example

Display the port mirroring configuration.

```
<Huawei> display mirror-port
------------------------------------------------------------------------------
  Mirror-port             Direction  Observe-dest
------------------------------------------------------------------------------
1 Ethernet2/0/0           Inbound    Ethernet2/0/1
2 GigabitEthernet1/0/0    Inbound    DIP:2.1.1.2 SIP:1.1.1.2 DSCP:0
------------------------------------------------------------------------------
```

Table 21-64 Description of the display mirror-port command output

Item	Description
Mirror-port	Mirrored ports. You can run the **21.10.3 mirror (interface view)** command to set this parameter.
Direction	Direction of packets on a mirrored port. The value can be: • both: indicates incoming and outgoing packets. • inbound: indicates incoming packets. • outbound: indicates outgoing packets. You can run the **21.10.3 mirror (interface view)** command to set this parameter.
Observe-dest	Local observing port. You can run the **21.10.5 observe-port** command to set local observing port.

Related Topics

21.10.3 mirror (interface view)

21.10.5 observe-port

Copyright © Huawei Technologies Co., Ltd.

21.10.2 display observe-port

Function

The **display observe-port** command displays the observing port configuration.

Format

display observe-port

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the observing port configuration.

```
<Huawei> display observe-port
  ------------------------------------------------------------------------
  Index    : 1
  Interface: Ethernet1/0/1
  Used     : 1
  ------------------------------------------------------------------------
```

Table 21-65 Description of the display observe-port command output

Item	Description
Index	Index of the observing port.
Interface	Observing port. You can run the **21.10.5 observe-port** command to set this parameter.
Used	Number of times that the observing port is used.

Related Topics

21.10.5 observe-port

Copyright © Huawei Technologies Co., Ltd.

21.10.3 mirror (interface view)

Function

The **mirror** command enables port mirroring.

The **undo mirror** command disables port mirroring.

By default, port mirroring is disabled.

Format

mirror to observe-port { **both** | **inbound** | **outbound** } [**exclude-link-head**]

undo mirror { **both** | **inbound** | **outbound** }

Parameters

Parameter	Description	Value
observe-port	Indicates local port mirroring.	-
both	Mirrors both the incoming and outgoing packets on a port.	-
inbound	Mirrors only incoming packets on a port.	-
outbound	Mirrors only outgoing packets on a port.	-
exclude-link-head	Removes non-Ethernet link layer information before mirroring packets on a port.	-

Views

Interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device supports mirroring incoming packets, outgoing packets, and both incoming and outgoing packets.

The device may fail to analyze some IP packets that carry non-Ethernet link layer information, such as IPOA packets during port mirroring. In this case, specify the

 Copyright © Huawei Technologies Co., Ltd.

exclude-link-layer parameter to remove non-Ethernet link layer information from the packets, so that the device can correctly analyze the packets.

Prerequisites

In local port mirroring, the local observing port has been configured using the **21.10.5 observe-port** command.

Precautions

- An observing port or server can be applied to port mirroring and traffic mirroring simultaneously. However, you cannot identify the source of mirrored packets by using the **5.1.4 display interface** command.
- Port mirroring does not affect system security but affects system performance. To ensure system performance, disable port mirroring when you do not need to monitor traffic.
- To configure mirroring on a port again, run the **undo mirror** { **both** | **inbound** | **outbound** } command to delete the existing configuration first.
- To ensure that all mirrored packets are transmitted to the observing port, configure the same link type and bandwidth for the mirrored and observing ports.

Example

Mirror all incoming packets on Eth2/0/0 to the observing port.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] mirror to observe-port inbound
```

Related Topics

21.10.5 observe-port

21.10.4 mirror (traffic behavior view)

Function

The **mirror** command used in the traffic behavior view enables traffic mirroring to mirror packets matching certain rules to the observing port.

The **undo mirror** command disables traffic mirroring.

By default, traffic mirroring is disabled.

Format

mirror to observe-port

undo mirror

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
observe-port	Indicates the observing port used for traffic mirroring.	-

Views

Traffic behavior view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a traffic policy containing a traffic behavior is configured on a port, the device mirrors the packets that match the traffic policy to the local observing port or remote observing server. The local observing port must be a LAN-side port.

Prerequisites

- A traffic behavior has been created using the **20.1.44 traffic behavior** command.
- In local traffic mirroring, the local observing port has been configured using the **21.10.5 observe-port** command.

Follow-up Procedure

Create a traffic classifier and a traffic policy, bind the traffic classifier and traffic behavior to the traffic policy, and apply the traffic policy to the mirrored port.

Precautions

- An observing port or server can be applied to port mirroring and traffic mirroring simultaneously. However, you cannot identify the source of mirrored packets by using the **5.1.4 display interface** command.
- Traffic mirroring does not affect system security but affects system performance. To ensure system performance, disable traffic mirroring when you do not need to monitor traffic.

Example

Mirror the packets matching certain rules to the observing port.

```
<Huawei> system-view
[Huawei] traffic behavior tb1
[Huawei-behavior-tb1] mirror to observe-port
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

20.1.44 traffic behavior
21.10.5 observe-port

21.10.5 observe-port

Function

The **observe-port** command configures a local observing port.

The **undo observe-port** command deletes a local observing port.

By default, no local observing port is configured.

NOTE

In PPPoEoA and IPoEoA scenarios, only WAN-side interfaces can be used as observing interfaces.

Format

observe-port interface *interface-type interface-number*

undo observe-port

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the observing port. • *interface-type* specifies the type of the port. • *interface-number* specifies the number of the port.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the monitoring device and monitored device are connected to the same router, run the **observe-port** command to configure a local observing port to monitor

Copyright © Huawei Technologies Co., Ltd.

ports on the monitored device or traffic passing through the ports on the monitored device.

Precautions

- Do not configure other functions on an observing port; otherwise, the mirroring function is affected.
- If an observing port configured with the mirroring function needs to be deleted, delete the mirrored port first.
- The management port cannot be configured as a local observing port.
- Only LAN-side and WAN-side ports can be configured as local observing ports.

Example

Configure Eth2/0/0 as the local observing port.

```
<Huawei> system-view
[Huawei] observe-port interface ethernet 2/0/0
```

Related Topics

21.10.2 display observe-port

21.11 Packet Capture Configuration Command

NOTE

Based on your requirements to detect failures in telecom transmission, this feature may collect or store some communication information about specific customers. Huawei cannot offer services to collect or store this information unilaterally. Before enabling the function, ensure that it is performed within the boundaries permitted by applicable laws and regulations. Effective measures must be taken to ensure that information is securely protected.

21.11.1 capture-packet

Function

The **capture-packet** command captures service packets matching specified rules, displays captured packet information on the terminal, or saves the captured packets on the local device.

By default, the captured packets on the device are not configured.

Format

capture-packet { **interface** *interface-type interface-number* | **dsp** } [**acl** *acl-number*] **destination** { **terminal** | **file** *file-name* } * [**car cir** *car-value* | **time-out** *time* | **packet-num** *number* | **packet-len** *length* }] *

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Captures packets on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
dsp	Specifies the captured DSP voice packets.	-
acl	Configures an ACL.	-
acl-number	Captures packets matching a specified ACL.	The value is an integer that ranges from 2000 to 4999.
destination	Indicates the destination to which captured packet information is sent.	-
terminal	Displays captured packet information on a terminal.	-
file *file-name*	Saves captured packet information to a file. *file-name* is in the format of [drive][file-name] (such as flash:/test.cap), in which [file-name] is in the format of *.cap.	The value is a string of 5 to 63 characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
car cir *car-value*	Specifies the rate at which packets are captured.	The value is an integer that ranges from 1 to 256, in pps. The default value is 64 pps.
time-out *time*	Specifies the timeout period for capturing packets. The system stops capturing packets after the specified timeout period expires.	The value is an integer that ranges from 1 to 300, in seconds. By default, the timeout period is 60s.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
packet-num *number*	Specifies the number of packets to be captured. The system stops capturing packets after the specified number of packets are captured.	The value is an integer that ranges from 1 to 2000. The default value is 100.
packet-len *length*	Specifies the length of captured packets that can be displayed on the terminal or stored on the storage medium.	The value is an integer that ranges from 20 to 64, in bytes. The default value is 64 bytes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If an error occurs in service traffic forwarding (for example, the traffic status does not match the traffic model), it is recommended that you configure the device to capture service packets for analysis so that the device can quickly identify invalid packets. This function ensures correct data transmission on the network.

Precautions

When packets are received by a LAN port and sent to a LAN port, the packets cannot be captured.

When the 8FE1GE or 24GE board is installed on an AR1220, Layer 2 packets cannot be captured, and Layer 3 packets can be captured. When the 8FE1GE or 24GE board is installed on a model except AR1220 and the inbound interface is on 8FE1GE or 24GE, both Layer 2 and Layer 3 packets are forwarded by LSW, and the packets cannot be mirrored. When the inbound interface is on another LAN board, Layer 2 packets cannot be mirrored and Layer 3 packets can be mirrored.

The device can capture incoming and outgoing packets.

Before using the **capture-packet** command again, wait until the last command execution is complete.

The system limits the rate of captured packets. If the rate of packets exceeds the limit, some packets may be discarded.

You can set the timeout period specified by *time* and the number of packets to be captured specified by *number* for a capture instance. If the timeout period expires

 Copyright © Huawei Technologies Co., Ltd.

or the specified number of packets are captured, the system stops capturing packets.

The **capture-packet** and **voice-monitor** commands cannot be configured simultaneously.

Example

Capture packets on the interface GE1/0/0 and display them on the terminal.

```
<Huawei> system-view
[Huawei] capture-packet interface gigabitethernet 1/0/0 destination terminal time-out 10
[Huawei]
 Packet: 1
 ----------------------------------------------------------
 ff ff ff ff ff ff 00 e0 fc 01 00 08 08 06 00 01
 08 00 06 04 00 01 00 e0 fc 01 00 08 02 01 01 03
 00 00 00 00 00 00 0a 01 01 01 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00
 ----------------------------------------------------------

 ------------------capture report-----------------------
 file: NULL
 interface: GigabitEthernet1/0/0
 acl: -
 car: 64pps timeout: 10s
 packets: 100 (expected) 1 (actual)
 length: 48 (expected)
 ----------------------------------------------------------
```

Table 21-66 Description of the capture-packet command output

Item	Description
file	Local path that stores captured packets. NULL marking for empty.
interface	Interface where packets are captured.
acl	ACL number.
car	Rate of captured packets.
timeout	Timeout interval of packet capture. The system stops capturing packets after the specified time interval.
packets	Expected number and actual number of captured packets.
length	Length of captured packets.

21.11.2 display voice-monitor

Function

The **display voice-monitor** command displays information about voice packets passing the device.

Copyright © Huawei Technologies Co., Ltd.

Format

display voice-monitor

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To view information about voice packets passing the device, run the **display voice-monitor** command.

Prerequisites

The device is configured to capture voice packets using the **voice-monitor** command.

Example

Display information about voice packets passing the device.

```
<Huawei> display voice-monitor
-------------------------------------------------------------------------
TelNo                IPAddr         Port      Direction RuleIndex
-------------------------------------------------------------------------
20000                10.0.0.1       51201     Inbound   0
10000                10.0.0.2       61945     Outbound  1
```

Table 21-67 Description of the display voice-monitor command output

Item	Description
TelNo	Phone number in the captured voice packets.
IPAddr	IP address of voice packets.
Port	Port number of voice packets.
Direction	Direction of voice packets: • Inbound: incoming voice packets. • Outbound: outgoing voice packets.
RuleIndex	ID of the resource occupied by voice packets.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.11.3 voice-monitor

21.11.3 voice-monitor

Function

The **voice-monitor** command configures the device to capture voice packets passing the device and save them.

By default, the device is not configured to capture voice packets passing the device.

Format

voice-monitor interface *interface-type interface-number* **destination file** *file-name* * **telno** *telephone-number* &<1-8> [**car cir** *cir-value* | **time-out** *time* | **packet-num** *number*] | **packet-len** *length* } *

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Captures packets on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
destination	Specifies the destination where captured packets are saved.	-
file *file-name*	Specifies the name of the file for storing captured packets.	The value is a string of 5 to 63 characters without spaces. The value must end with *.cap.
telno *telephone-number* &<1-8>	Specifies the phone number in captured packets.	The value is a string of 1 to 24 numerals. Each numeral ranges from 0 to 9. A maximum of 8 telephone numbers can be entered.
car cir *cir-value*	Specifies the rate at which packets are captured.	The value is an integer that ranges from 1 to 256, in pps. The default rate is 64 pps.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
time-out *time*	Specifies the timeout interval of packet capture. The system stops capturing packets after the specified timeout interval.	The value is an integer that ranges from 1 to 300, in seconds. The default timeout interval is 60s.
packet-num *number*	Specifies the number of packets to be captured. The system stops capturing packets after the specified number of packets are captured.	The value is an integer that ranges from 1 to 2000. The default value is 100.
packet-len *length*	Specifies the length of captured packets that can be displayed on the terminal or stored on the storage medium.	The value is an integer that ranges from 20 to 64, in bytes. The default value is 64 bytes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When unexpected voice traffic occurs, for example, the traffic status does not match the traffic model, run the **voice-monitor** command to configure the device to capture voice packets for analysis. Then the device can process invalid packets in a timely manner, and data services can be correctly transmitted and voice communication quality is ensured.

When configuring packet capture, you can set parameters according to the number of packets on an interface. If there are many packets on the interface, set a small value of *time* and a large value of *number*. If there are less packets on an interface, set a large value of *time* and a small value of *number*.

Precautions

- The packet capture configuration is not saved in the configuration file, and becomes invalid when packet capture is complete.
- Before using the **voice-monitor** command again, wait until the last command execution is complete.
- The system limits the rate of captured packets. If the rate of packets exceeds the limit, some packets may be discarded.

 Copyright © Huawei Technologies Co., Ltd.

- You can set the timeout interval of packet capture and number of packets to be captured. The system stops capturing packets after the timeout interval or the number of packets to be captured is reached.
- The **voice-monitor** and **capture-packet** commands cannot be configured simultaneously.

Example

Configure the device to capture voice packets on GE1/0/0 and save them in the **capture.cap** file.

```
<Huawei> system-view
[Huawei] voice-monitor interface gigabitethernet 1/0/0 destination file capture.cap telno 10000 20000
Warning: The packet capture function has been enabled and packets are stored in flash:/capture.cap .
[Huawei]
  ------------------capture report-----------------------
  file: flash:/capture.cap
  interface: GigabitEthernet1/0/0
  acl: -
  car: 64pps timeout: 60s
  packets: 100 (expected) 0 (actual)
  length: whole (expected)
  ------------------------------------------------------
```

Table 21-68 Description of the voice-monitor command output

Item	Description
file	File name and path for storing captured packets.
interface	Interface where packets are captured.
acl	ACL number.
car	Rate at which packets are captured.
timeout	Timeout interval of packet capture. The system stops capturing packets after the specified timeout interval.
packets	Expected and actual numbers of captured packets.
length	Length of captured packets.

21.12 NetStream Configuration Commands

NOTE

- The NetStream function conforms to IETF RFC3954. For security risks, see IETF RFC3954. This function involves analyzing the communications information of terminal customers. Before enabling the function, ensure that it is performed within the boundaries permitted by applicable laws and regulations. Effective measures must be taken to ensure that information is securely protected.
- NetStream supports sampling of IPv4 unicast, multicast packets, and IPv4 packets encapsulated with MPLS labels.

Copyright © Huawei Technologies Co., Ltd.

21.12.1 collect application

Function

The **collect application** command configures the application name or description of traffic to be added to the flexible flow statistics exported to the NSC.

The **undo collect application** command restores the default configuration.

By default, the flexible flow statistics that are exported to the NSC do not contain the application name and description.

Format

collect application { **name** | **description** }

undo collect application { **name** | **description** }

Parameters

Parameter	Description	Value
name	Specifies the traffic application name to be added to the flexible flow statistics exported to the NSC.	-
description	Specifies the traffic description to be added to the flexible flow statistics exported to the NSC.	-

Views

Flexible flow template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain more information from flexible flow statistics, you can specify that the statistics contain the application name or description of traffic and set the application names and description according to your needs.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The **engine enable** command has been run to enable deep security defense, and the **sa application-statistic enable** command has been run to enable SA statistics collection on a NetStream interface.

After the deep security function is enabled, if SAC is used for the first time, run the **update restore sdb-default** command to manually load the SA signature file.

Example

Specify the traffic application name to be added to the flexible flow statistics exported to the NSC.

```
<Huawei> system-view
[Huawei] ip netstream record huawei_record
[Huawei-record-huawei_record] collect application name
```

21.12.2 collect category name

Function

The **collect category name** command configures the application category and subcategory of traffic to be added to the flexible flow statistics exported to the NSC.

The **undo collect category name** command restores the default configuration.

By default, the flexible flow statistics that are exported to the NSC do not contain the application category and subcategory.

Format

collect category name

undo collect category name

Parameters

None

Views

Flexible flow template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain more information from flexible flow statistics, you can specify that the statistics contain the application name or description of traffic and set the application names and description according to your needs.

Prerequisites

Copyright © Huawei Technologies Co., Ltd.

The **engine enable** command has been run to enable deep security defense, and the **sa application-statistic enable** command has been run to enable SA statistics collection on a NetStream interface.

After the deep security function is enabled, if SAC is used for the first time, run the **update restore sdb-default** command to manually load the SA signature file.

Example

Specify that the flexible flow statistics that are exported to the NSC contain the application category and subcategory of traffic.

```
<Huawei> system-view
[Huawei] ip netstream record huawei_record
[Huawei-record-huawei_record] collect category name
```

21.12.3 collect counter

Function

The **collect counter** command allows the flexible flow statistics exported to the NetStream Collector (NSC) to contain the number of bytes and packets.

The **undo collect counter** command restores the default setting.

By default, the flexible flow statistics exported to the NSC do not contain the number of bytes or packets.

Format

collect counter { **bytes** | **packets** }

undo collect counter { **bytes** | **packets** }

Parameters

Parameter	Description	Value
bytes	Indicates that the flexible flow statistics exported to NSC contain the number of bytes.	-
packets	Indicates that the flexible flow statistics exported to NSC contain the number of packets.	-

Views

Flexible flow statistics template view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain richer flow statistics, configure whether flexible flow statistics contain the number of bytes and packets.

Prerequisites

A flexible flow statistics template has been created using the **ip netstream record** command.

Precaution

If a flexible flow statistics template has been applied to an interface, the template configuration cannot be modified or deleted.

Example

Configure the flexible flow statistics template **record1** to export the flexible flow statistics containing the number of packets to the NSC.

```
<Huawei> system-view
[Huawei] ip netstream record record1
[Huawei-record-record1] collect counter packets
```

Related Topics

21.12.29 ip netstream record

21.12.4 collect interface

Function

The **collect interface** command allows the flexible flow statistics exported to the NSC to contain the indexes of inbound and outbound interfaces.

The **undo collect interface** command restores the default setting.

By default, the flexible flow statistics exported to the NSC do not contain the index of inbound or outbound interface.

Format

collect interface { **input** | **output** }

undo collect interface { **input** | **output** }

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
input	Indicates that the flexible flow statistics exported to the NSC contain the index of inbound interface.	-
output	Indicates that the flexible flow statistics exported to the NSC contain the index of outbound interface.	-

Views

Flexible flow statistics template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain richer flow statistics, configure whether flexible flow statistics exported to the NSC contain indexes of inbound and outbound interfaces.

Prerequisites

A flexible flow statistics template has been created using the **ip netstream record** command.

Precaution

If a flexible flow statistics template has been applied to an interface, the template configuration cannot be modified or deleted.

Example

Configure the flexible flow statistics template **record1** to export the flexible flow statistics containing the inbound interface index to the NSC.

```
<Huawei> system-view
[Huawei] ip netstream record record1
[Huawei-record-record1] collect interface input
```

Related Topics

21.12.29 ip netstream record

 Copyright © Huawei Technologies Co., Ltd.

21.12.5 display ip netstream

Function

The **display ip netstream** command displays the NetStream configurations.

Format

display ip netstream { **all** | **global** }

Parameters

Parameter	Description	Value
all	Displays all the NetStream configurations, including: • NetStream configurations in the system view • NetStream configurations in the aggregation view • NetStream configurations in the flexible flow statistics view • NetStream configurations in the interface view	-
global	Displays the NetStream configurations in a specified view, for example: • NetStream configurations in the system view • NetStream configurations in the aggregation view • NetStream configurations in the flexible flow statistics view	-

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

None

Example

Display NetStream configurations in the system view and aggregation view.

```
<Huawei> display ip netstream global
ip netstream export host 10.0.0.2 255 vpn-instance vpna
ip netstream aggregation destination-prefix
 enable
 export version 9
 ip netstream export host 10.5.5.5 3 vpn-instance vpna
```

Table 21-69 Description of the display ip netstream global command output

Item	Description
ip netstream export host *ip-address port-number* vpn-instance *vpn-instance-name*	The field *ip-address* indicates the destination address of the exported packets, and *port-number* is the UDP port. The field *vpn-instance-name* indicates the VPN instance to which the destination address belongs. This field is displayed only when the **ip netstream export host** command has been executed in the system view.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
ip netstream aggregation destination-prefix	Destination-prefix aggregation method. This field is displayed only when the **ip netstream aggregation** command has been executed to set the aggregation method. Currently, the following aggregation modes are supported: • as: AS aggregation • as-tos: AS-ToS aggregation • destination-prefix: destination-prefix aggregation • destination-prefix-tos: destination-prefix-ToS aggregation • prefix: prefix aggregation • prefix-tos: prefix-ToS aggregation • protocol-port: protocol-port aggregation • protocol-port-tos: protocol-port-ToS aggregation • source-prefix: source-prefix aggregation • source-prefix-tos: source-prefix-ToS aggregation
enable	The destination-prefix aggregation mode is enabled. This field is displayed only when the **enable** command has been executed in the aggregation view.
export version *version*	The field *version* indicates the version format of the exported packets carrying aggregation flow statistics. If the version retains the default setting, this field is not displayed. This field is displayed only when the **export version** command has been executed.
ip netstream export host *ip-address port-number* vpn-instance *vpn-instance-name*	The field *ip-address* indicates the destination address of the exported packets, and *port-number* is the UDP port. The field *vpn-instance-name* indicates the VPN instance to which the destination address belongs. This field is displayed only when the **ip netstream export host** command has been executed in the NetStream aggregation view.

Related Topics

21.12.14 ip netstream aggregation
21.12.21 ip netstream export host
21.12.26 ip netstream export version

Copyright © Huawei Technologies Co., Ltd.

21.12.11 enable

21.12.6 display ip netstream cache

Function

The **display ip netstream cache** command displays flow information in the NetStream cache.

Format

display ip netstream cache [**classify** [**source-ip** *source-ip* | **destination-ip** *destination-ip* | **source-port** *source-port* | **destination-port** *destination-port* | **protocol** *protocol-id* | **start-time** *start-time* | **end-time** *end-time*] * | [**verbose**] | **top** [*top-value*] [**sort-by** { **bytes** | **packets** }] | **verbose**]

Parameters

Parameter	Description	Value
classify	Searches for the saved flow entries.	-
source-ip *source-ip*	Specifies the source IP address used for search.	The value is in dotted decimal notation.
destination-ip *destination-ip*	Specifies the destination IP address used for search.	The value is in dotted decimal notation.
source-port *source-port*	Specifies the source port number used for search.	The value is an integer that ranges from 0 to 65535.
destination-port *destination-port*	Specifies the destination port number used for search.	The value is an integer that ranges from 0 to 65535.
protocol *protocol-id*	Specifies the protocol number used for search.	The value is an integer that ranges from 0 to 65535.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
start-time *start-time*	Specifies the start time used for search.	The value is in hh:mm:ss YYYY/MM/DD formats. The time is in 24-hour format and displayed as hh:mm:ss. hh indicates the hour that is an integer ranging from 0 to 23. mm indicates the minute that is an integer ranging from 0 to 59. ss indicates the second that is an integer ranging from 0 to 59. The date is in YYYY/MM/DD format. YYYY specifies the year, MM specifies the month, and DD specifies the day. The value is an integer that ranges from 1970-01-01 to 2099-12-31.
end-time *end-time*	Specifies the end time used for search.	The value is in hh:mm:ss YYYY/MM/DD formats. The time is in 24-hour format and displayed as hh:mm:ss. hh indicates the hour that is an integer ranging from 0 to 23. mm indicates the minute that is an integer ranging from 0 to 59. ss indicates the second that is an integer ranging from 0 to 59. The date is in YYYY/MM/DD format. YYYY specifies the year, MM specifies the month, and DD specifies the day. The value is an integer that ranges from 1970-01-01 to 2099-12-31.
top	Displays the flows in the descending order of flow volume. By default, flows are displayed in the descending order of the number of packets.	-
top-value	Specifies the number of flows that need to be displayed in a certain order.	The value is an integer that ranges from 1 to 200. The default value is 10.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
sort-by	Specifies the order in which flows are displayed.	-
bytes	Indicates that the flows are displayed in the order of bytes.	-
packets	Indicates that the flows are displayed in the order of packets.	-
verbose	Displays detailed information about flows in the NetStream cache.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the NetStream sampling function is enabled, run the **display ip netstream cache** command to view information about flows in NetStream cache.

To view the cached flows in the order of flow volume, run the **display ip netstream cache top** command. The **display ip netstream cache** command can display the flows in the descending order of the number of **bytes** or **packets**.

To search for the saved flow entries based on the seven attributes (including the source IP address, destination IP address, source port number, destination port number, protocol number, start time, and end time), run the **display ip netstream cache classify** command.

NOTE

Only AR2204E, AR2240, AR2240C, and AR3200 series routers support flow entry search based on the seven attributes.

Precaution

This command cannot display the aged flows, so you must run this command before the flows age in the cache.

The flow table information is based on seven-tuple to retrieve sequential dependent relationships. For example, after retrieval based on the destination IP

 Copyright © Huawei Technologies Co., Ltd.

address, the source port number, destination port number, protocol number, and start or end time can also be retrieved, but the source IP address cannot be retrieved.

When the number of data flows on the network exceeds the upper limit, an accelerated aging mechanism can be used so that statistics about all data flows can be collected.

- When the number of remaining flow tables is between 25% and 30% of the upper limit, the actual inactive aging period is two thirds of the configured inactive aging period.
- When the number of remaining flow tables is greater than 5% of the upper limit and less than or equal to 25% of the upper limit, the actual inactive aging period is half of the configured inactive aging period.
- When the number of remaining flow tables is less than or equal to 5% of the upper limit, the flow tables are aged after the aging timer expires.

Example

Display information about flows in the NetStream cache.

```
<Huawei> display ip netstream cache
 IP netstream cache information :
   Active stream timeout ( in minutes )   : 30
   Inactive stream timeout ( in seconds ) : 30
   IP active stream number                : 2
   IP inactive stream number              : 0
   Last statistics reset time             : Never

IP packet size distribution (41100 total packets) :
 1-32   64   96  128  160  192  224  256  288  320  352  384  416  448
.000 .000 .148 .000 .850 .000 .000 .000 .000 .000 .000 .000 .000 .000

  480  512  544  576 1024 1536 2048 2506 3072 3584 4096 4608 >4608
.000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

 Protocol          Total   Packets    Stream    Packets  Active(sec)  Idle(sec)
                  Streams     /sec     /sec    /stream    /stream     /stream
-------------------------------------------------------------------------------
 IP-other              1       928        0       6500          7           0
 UDP-other             1       300        0      35100        117           0

Type  DstIP(Port)           SrcIP(Port)          Pro  ToS  Packets      If(Direc)
-------------------------------------------------------------------------------
IP    192.168.1.2(80)         192.168.2.2(0)         17   0    353
GigabitEthernet0/0/0(I)
IP    192.168.2.2(0)          192.168.1.2(0)         114  68   70     GigabitEthernet0/0/0(O)
```

Table 21-70 Description of the display ip NetStream cache command output

Item	Description
IP netstream cache information	Information about the NetStream cache.
Active stream timeout (in minutes)	Active aging time, in minutes.
Inactive stream timeout (in seconds)	Inactive aging time, in seconds.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
IP active stream number	Number of active IP flows in the NetStream cache.
IP inactive stream number	Number of inactive IP flows in the NetStream cache.
Last statistics reset time	Last time the statistics are cleared. This time does not change with the system time. This field is displayed only when the **reset ip netstream statistic** command is executed; otherwise, the message "Last statistics reset time : Never" is displayed.
IP packet size distribution (41100 total packets)	Distribution of IP packets based on the packet size. Bracketed information indicates the total number of IP packets. The distribution value is displayed as a three-bit decimal based on the ratio to the total number of IP packets. For example, ".027" indicates that the IP packets in the NetStream cache are 0.027 of the total number of IP packets.
1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480 512 544 576 1024 1536 2048 2506 3072 3584 4096 4608 >4608	Interval between IP packet size. The packet length does not contain the link layer header. When the packet length does not exceed 576 bytes, the packet length increases by 32 bytes. For example, "1-32" maps the number of packets whose lengths range from 1 byte to 32 bytes, and "64" maps the number of packets whose lengths range from 33 bytes to 64 bytes. When the packet length exceeds 1024 bytes, the packet length increases by 512 bytes. For example, "1536" maps the number of packets whose lengths range from 1025 bytes to 1536 bytes. The number of packets whose lengths range from 577 bytes to 1024 bytes is recorded mapping "1024".
Protocol	Protocol number.
Total Streams	Total number of flows.
Packets/sec	Number of packets per second.
Stream/sec	Number of flows per second.
Packets /stream	Average number of packets in each flow.
Active(sec) /stream	Average active time of each flow. Unit is seconds.
Idle(sec) /stream	Average inactive time of each flow. Unit is seconds.
Type	Flow type.
DstIP(Port)	Destination IP address (destination port number) of flows.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
SrcIP(Port)	Source IP address (source port number) of flows.
Pro	Protocol type of flows.
ToS	Service type of flows.
Pkts	Number of packets in a flow.
If(Direc)	Interface name (flow direction). • (I): inbound direction • (O): outbound direction

21.12.7 display ip netstream record

Function

The **display ip netstream record** command displays the configuration of a flexible flow statistics template.

Format

display ip netstream record { **all** | **name** *record-name* }

Parameters

Parameter	Description	Value
all	Displays configurations of all flexible flow statistics templates.	-
name *record-name*	Displays the configuration of a flexible flow statistics template specified by *record-name*.	**NOTE** The parameter *record-name* is determined by the template name configured using the **ip netstream record** command.

Views

All views

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Display the configuration of the flexible flow statistics template **test0**.

```
<Huawei> display ip netstream record name test0
ip netstream record test0
 match ipv4 source-address
 match ipv4 destination-address
```

Table 21-71 Description of the display ip netstream record command output

Item	Description
ip netstream record test0	The flexible flow statistics template is **test0**.
match ipv4 source-address	According to the template **test0**, flows are aggregated based on the source IP address. This field is configured using the **match ipv4** command.
match ipv4 destination-address	According to the template **test0**, flows are aggregated based on the destination IP address. This field is configured using the **match ipv4** command.

Related Topics

21.12.29 ip netstream record

21.12.8 display ip netstream statistic

Function

The **display ip netstream statistic** command displays the NetStream flow statistics.

Format

display ip netstream statistic

Parameters

None

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

None

Example

Display the NetStream statistics.

```
<Huawei> display ip netstream statistic
 Origin ingress entries           : 30000
 Origin ingress packets           : 30000
 Origin ingress octets            : 1380000
 Origin egress entries            : 0
 Origin egress packets            : 0
 Origin egress octets             : 0
 Origin total entries             : 30000
 Agility ingress entries          : 30000
 Agility ingress packets          : 30000
 Agility ingress octets           : 3960000
 Agility egress entries           : 0
 Agility egress packets           : 0
 Agility egress octets            : 0
 Agility total entries            : 30000
 Handle origin entries            : 29035
 Handle agility entries           : 29050
 Handle As aggre entries          : 1
 Handle ProtPort aggre entries    : 1
 Handle SrcPrefix aggre entries   : 118
 Handle DstPrefix aggre entries   : 1
 Handle Prefix aggre entries      : 118
 Handle AsTos aggre entries       : 1
 Handle ProtPortTos aggre entries : 1
 Handle SrcPreTos aggre entries   : 118
 Handle DstPreTos aggre entries   : 1
 Handle PreTos aggre entries      : 118
```

Table 21-72 Description of the display ip netstream statistic command output

Item	Description
Origin ingress entries	Total number of incoming original flows.
Origin ingress packets	Total number of incoming original packets.
Origin ingress octets	Total number of incoming original bytes.
Origin egress entries	Total number of outgoing original flows.
Origin egress packets	Total number of outgoing original packets.
Origin egress octets	Total number of outgoing original bytes.
Origin total entries	Total number of original flows.
Agility ingress entries	Number of incoming flexible flows.
Agility ingress packets	Number of incoming flexible packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Agility ingress octets	Number of incoming flexible bytes.
Agility egress entries	Number of outgoing flexible flows.
Agility egress packets	Number of outgoing flexible packets.
Agility egress octets	Number of outgoing flexible bytes.
Agility total entries	Total number of flexible flows.
Handle origin entries	Number of processed incoming and outgoing original flows.
Handle agility entries	Number of processed incoming and outgoing flexible flows.
Handle As aggre entries	Number of processed incoming and outgoing AS aggregation flows.
Handle ProtPort aggre entries	Number of processed incoming and outgoing protocol-port aggregation flows.
Handle SrcPrefix aggre entries	Number of processed incoming and outgoing source-prefix aggregation flows.
Handle DstPrefix aggre entries	Number of processed incoming and outgoing destination-prefix aggregation flows.
Handle Prefix aggre entries	Number of processed incoming and outgoing prefix aggregation flows.
Handle AsTos aggre entries	Number of processed incoming and outgoing AS-ToS aggregation flows.
Handle ProtPortTos aggre entries	Number of processed incoming and outgoing protocol-port-ToS aggregation flows.
Handle SrcPreTos aggre entries	Number of processed incoming and outgoing source-prefix-ToS aggregation flows.
Handle DstPreTos aggre entries	Number of processed incoming and outgoing destination-prefix-ToS aggregation flows.
Handle PreTos aggre entries	Number of processed incoming and outgoing prefix-ToS aggregation flows.

21.12.9 display snmp-agent trap feature-name netstream all

Function

The **display snmp-agent trap feature-name netstream all** command displays the status of all traps on the NetStream module.

 Copyright © Huawei Technologies Co., Ltd.

Format

display snmp-agent trap feature-name netstream all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display snmp-agent trap feature-name netstream all** command to check the status of all traps on the NetStream module. This status can be configured using the **snmp-agent trap enable feature-name netstream** command.

Example

Display the status of all traps on the NetStream module.

```
<Huawei> display snmp-agent trap feature-name netstream all
------------------------------------------------------------------------------
Feature name: netstream
Trap number : 1
------------------------------------------------------------------------------
Trap name                 Default switch status   Current switch status
hwNetStreamSessionFull          off                     off
```

Table 21-73 Description of the display snmp-agent trap feature-name netstream all command output

Item	Description
Feature name	Name of the module that a trap message belongs.
Trap number	Number of trap messages.
Trap name	Name of a trap.
Default switch status	Default status of a trap: • on: The trap is enabled. • off: The trap is disabled.
Current switch status	Status of a trap: • on: The trap is enabled. • off: The trap is disabled. This status can be configured using the **snmp-agent trap enable feature-name netstream** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
hwNetStreamSessionFull	The NetStream session table is full.

Related Topics

21.12.44 snmp-agent trap enable feature-name netstream

21.12.10 display snmp-agent trap feature-name sindex all

Function

The **display snmp-agent trap feature-name sindex all** command displays the status of all traps on the SINDEX module.

Format

display snmp-agent trap feature-name sindex all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display snmp-agent trap feature-name sindex all** command to check the status of all traps on the SINDEX module. This status can be configured using the **snmp-agent trap enable feature-name sindex** command.

Example

Display the status of all traps on the SINDEX module.

```
<Huawei> display snmp-agent trap feature-name sindex all
------------------------------------------------------------------------------
Feature name: SINDEX
Trap number : 1
------------------------------------------------------------------------------
Trap name                     Default switch status   Current switch status
hwNetStreamIndexUsedUp        on                      on
```


Copyright © Huawei Technologies Co., Ltd.

Table 21-74 Description of the display snmp-agent trap feature-name sindex all command output

Item	Description
Feature name	Name of the module that a trap message belongs.
Trap number	Number of trap messages.
Trap name	Name of a trap.
Default switch status	Default status of a trap: • on: The trap is enabled. • off: The trap is disabled.
Current switch status	Status of a trap: • on: The trap is enabled. • off: The trap is disabled. This status can be configured using the **snmp-agent trap enable feature-name sindex** command.
hwNetStreamIndexUsed-Up	The NetStream interface indexes are all allocated.

Related Topics

21.12.45 snmp-agent trap enable feature-name sindex

21.12.11 enable

Function

The **enable** command enables the aggregation function in the aggregation view.

The **undo enable** command disables the aggregation function in the aggregation view.

By default, the aggregation function is disabled.

Format

enable

undo enable

Parameters

None

Views

NetStream aggregation view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **enable** command takes effect only in the NetStream aggregation view. Flow statistics are exported according to the configured aggregation method only after you run the **enable** command in the aggregation view.

Precautions

When this command is executed, the device will send an aggregation template to the server.

Example

Enable destination address prefix aggregation.

```
<Huawei> system-view
[Huawei] ip netstream aggregation destination-prefix
[Huawei-aggregation-dstpre] enable
```

Related Topics

21.12.14 ip netstream aggregation

21.12.12 export version

Function

The **export version** command configures the versions of exported packets carrying aggregation flow statistics and flexible flow statistics.

The **undo export version** command restores the default setting.

By default, the version of exported packets carrying aggregation flow statistics is V8 and the version of exported packets carrying flexible flow statistics is V9.

Format

export version *version*

undo export version

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
version	Specifies the version numbers of exported packets carrying aggregation flow statistics and flexible flow statistics.	The value of *version* is as follows: • The value is 8, 9, or 10 in the NetStream aggregation view. The default is 8. • The value is 9 or 10 in the flexible flow statistics template view. The default is 9.

Views

NetStream aggregation view, flexible flow statistics template view

Default Level

3: Management level

Usage Guidelines

The NDE exports NetStream flow statistics to the NSC. The version of exported packets must be the same as that configured on the NSC so that the NSC can parse the exported packets.

The format of exported packets in V8 is fixed and is not easy to expand. The format of exported packets in V9 or V10 is defined in templates and is easy to combine or expand. The statistics are exported more flexibly.

Example

Set the version number of exported packets carrying aggregation flow statistics to V9.

```
<Huawei> system-view
[Huawei] ip netstream aggregation as
[Huawei-aggregation-as] export version 9
```

Set the version number of exported packets carrying flexible flow statistics to V10.

```
<Huawei> system-view
[Huawei] ip netstream record test
[Huawei-record-test] export version 10
```

Related Topics

21.12.14 ip netstream aggregation

21.12.29 ip netstream record

Copyright © Huawei Technologies Co., Ltd.

21.12.13 ip netstream

Function

The **ip netstream** command enables IPv4 flow statistics collection on the inbound and outbound interfaces.

The **undo ip netstream** command restores the default setting.

By default, statistics collection for IPv4 flows is disabled on the inbound and outbound interfaces.

Format

ip netstream { **inbound** | **outbound** }

undo ip netstream { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Enables flow statistics collection on the inbound interface.	-
outbound	Enables flow statistics collection on the outbound interface.	-

Views

Interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To export IPv4 flow statistics, you must run the **ip netstream** command to enable the IPv4 flow statistics collection function on the interface.

Precautions

When you enable the IPv4 flow statistics collection function on the inbound interface, enable the statistics collection function on unicast and multicast packets.

If the NetStream function is enabled on the main interface but you do not set a sampling ratio using the **21.12.31 ip netstream sampler (interface view)** command, the main interface uses the sampling ratio of 1:100. If you set the sampling ratio, the interface uses this sampling ratio.

Copyright © Huawei Technologies Co., Ltd.

When this command is executed, the device will send a template to the server.

Example

Enable the flow statistics collection function for the incoming IPv4 packets on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip netstream inbound
```

Related Topics

21.12.31 ip netstream sampler (interface view)

21.12.14 ip netstream aggregation

Function

The **ip netstream aggregation** command configures the aggregation method and displays the aggregation view.

Format

ip netstream aggregation { **as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** }

Parameters

Parameter	Description	Value
as	Specifies the AS aggregation. It classifies flows based on: • Source AS number • Destination AS number • Inbound interface index • Outbound interface index	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
as-tos	Specifies the AS-ToS aggregation. It classifies flows based on: • Source AS number • Destination AS number • Inbound interface index • Outbound interface index • ToS	-
destination-prefix	Specifies the destination-prefix aggregation. It classifies flows based on: • Destination AS number • Destination mask length • Outbound interface index • Destination prefix	-
destination-prefix-tos	Specifies the destination-prefix-ToS aggregation. It classifies flows based on: • Destination AS number • Destination mask length • Destination prefix • ToS • Outbound interface index	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
prefix	Specifies the prefix aggregation. It classifies flows based on: • Source and destination AS numbers • Source and destination mask lengths • Source and destination prefixes • Inbound interface index • Outbound interface index	-
prefix-tos	Specifies the prefix-ToS aggregation. It classifies flows based on: • Source and destination AS numbers • Source and destination mask lengths • Source and destination prefixes • ToS • Inbound interface index • Outbound interface index	-
protocol-port	Specifies the protocol-port aggregation. It classifies flows based on: • Protocol number • Source port number • Destination port number	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
protocol-port-tos	Specifies the protocol-port-ToS aggregation. It classifies flows based on: • Protocol number • Source port number • Destination port number • ToS • Inbound interface index • Outbound interface index	-
source-prefix	Specifies the source-prefix aggregation. It classifies flows based on: • Source AS number • Source mask length • Source prefix • Inbound interface index	-
source-prefix-tos	Specifies the source-prefix-ToS aggregation. It classifies flows based on: • Source AS number • Source mask length • Source prefix • ToS • Inbound interface index	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

NetStream aggregation groups the original flows with the same attributes together. The aggregation flow statistics collection and original flow statistics

 Copyright © Huawei Technologies Co., Ltd.

collection are different. The original flow statistics collection is on the basis of sampled packets, while the aggregation flow statistics collection is on the basis of original flows. Therefore, the aggregation flow statistics collection generates less data.

Follow-up Procedure

Run the **enable** command in the aggregation view to enable the device to export flow statistics according to the configured aggregation method.

Example

Configure the NetStream AS aggregation method.

```
<Huawei> system-view
[Huawei] ip netstream aggregation as
[Huawei-aggregation-as]
```

Configure the NetStream destination-prefix aggregation method.

```
<Huawei> system-view
[Huawei] ip netstream aggregation destination-prefix
[Huawei-aggregation-dstpre]
```

Related Topics

21.12.11 enable

21.12.15 ip netstream aggregation enable

Function

The **ip netstream aggregation enable** command enables the function of aggregating site visitor traffic on an interface.

The **undo ip netstream aggregation enable** command disables the function of aggregating site visitor traffic on an interface.

By default, the function of aggregating site visitor traffic is disabled on an interface.

Format

ip netstream aggregation enable

undo ip netstream aggregation enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **ip netstream aggregation enable** command to enable the function of aggregating site visitor traffic on an interface and report uplink and downlink data on the interface to the Agile Controller.

Example

Enable the function of aggregating site visitor traffic on an interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/0
[Huawei-Gigabitethernet0/0/0] ip netstream aggregation enable
```

21.12.16 ip netstream aggregation timeout active

Function

The **ip netstream aggregation timeout active** command sets the active aging time of aggregation flows.

The **undo ip netstream aggregation timeout active** command restores the default setting.

By default, the active aging time of aggregation flows is 30 minutes.

Format

ip netstream aggregation timeout active *active-interval*

undo ip netstream aggregation timeout active

Parameters

Parameter	Description	Value
active-interval	Specifies the active aging time of aggregation flows.	The value is an integer that ranges from 1 to 60, in minutes. The default value is 30.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Network traffic may burst intermittently, while the memory capacity of the NDE is limited. Earlier flows in the memory need to be exported to release space for the

Copyright © Huawei Technologies Co., Ltd.

new flows. The process of exporting old flows is called aging. All flows in the NDE memory will be exported to the NSC for analysis.

When the active time (from flow creation time to the current time) of an aggregation flow exceeds the specified active aging time, the flow is exported to the destination.

To quickly detect the status of an active flow, set the active time to a small value; however, this setting increases the frequency at which NetStream packets are sent. To reduce the frequency at which NetStream packets are exported and improve statistics collecting efficiency, set the active time to a large value.

Precaution

If you set multiple aging modes on the device, a flow is aged when it matches any criterion.

Example

Set the active aging time of aggregation flows to 20 minutes.

```
<Huawei> system-view
[Huawei] ip netstream aggregation timeout active 20
```

21.12.17 ip netstream aggregation timeout inactive

Function

The **ip netstream aggregation timeout inactive** command sets the inactive aging time of aggregation flows.

The **undo ip netstream aggregation timeout inactive** command restores the default setting.

By default, the inactive aging time of aggregation flows is 30 seconds.

Format

ip netstream aggregation timeout inactive *inactive-interval*

undo ip netstream aggregation timeout inactive

Parameters

Parameter	Description	Value
inactive-interval	Specifies the inactive aging time of aggregation flows.	The value is an integer that ranges from 10 to 600, in seconds. The default value is 30.

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Network traffic may burst intermittently, while the memory capacity of the NDE is limited. Earlier flows in the memory need to be exported to release space for the new flows. The process of exporting old flows is called aging. All flows in the NDE memory will be exported to the NSC for analysis.

When the inactive time (from the last packet receiving time to the current time) of an aggregation flow exceeds the specified inactive aging time, the flow is exported to the destination.

To quickly detect the status of an inactive flow, set the inactive time to a small value; however, this setting increases the frequency at which NetStream packets are sent. To reduce the frequency at which NetStream packets are exported and improve statistics collecting efficiency, set the inactive time to a large value.

Precaution

If you set multiple aging modes on the device, a flow is aged when it matches any criterion.

Example

Set the inactive aging time of aggregation flows to 40 seconds.

```
<Huawei> system-view
[Huawei] ip netstream aggregation timeout inactive 40
```

21.12.18 ip netstream as extend enable

Function

The **ip netstream as extend enable** command sets the BGP AS number range.

The **undo ip netstream as extend enable** command restores the default setting.

By default, the BGP AS numbers range from 1 to 65535.

Format

ip netstream as extend enable

undo ip netstream as extend enable

Parameters

None

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Management level

Usage Guidelines

Usage Scenario

By default, the BGP AS numbers range from 1 to 65535. A BGP AS number supports 32 bits; therefore, the BGP AS numbers ranging from 65536 to 4294967295 are not supported. After the **ip netstream as extend enable** command is executed, the BGP AS numbers ranging from 1 to 4294967295 can be supported.

Precautions

Only the output packets of V9 or V10 support the 32-bit BGP AS numbers.

Example

Set the supported BGP AS number range.

```
<Huawei> system-view
[Huawei] ip netstream as extend enable
```

21.12.19 ip netstream cache log enable

Function

The **ip netstream cache log enable** command enables the function of recording logs in NetStream traffic statistics globally.

The **undo ip netstream cache log enable** command disables the function of recording logs in NetStream traffic statistics globally.

By default, the function of recording logs is disabled.

NOTE

Only AR2204E&AR2240&AR2240C, and AR3200 Series do support the command.

Format

ip netstream cache log enable

undo ip netstream cache log enable

Parameters

None

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **ip netstream cache log enable** command to enable the function of recording logs in NetStream traffic statistics.

Prerequisites

Before running this command, you need to ensure that the valid path for storing logs in NetStream traffic statistics has been configured using the **ip netstream cache log log-directory** command.

Precautions

The device has a rate limit on recording flows, and a maximum of 8000 aging flows are supported in the aging period. If the number of aged flows exceeds 8000, the device may discard some flow records to protect CPU resources. You are advised to set a long aging time (the default value is recommended) to reduce the probability of flow record loss.

Example

Enable the function of recording logs in NetStream traffic statistics.

```
<Huawei> system-view
[Huawei] ip netstream cache log log-directory usb0:
[Huawei] ip netstream cache log enable
```

Related Topics

21.12.20 ip netstream cache log log-directory

21.12.20 ip netstream cache log log-directory

Function

The **ip netstream cache log log-directory** command sets the path for storing logs in NetStream traffic statistics.

The **undo ip netstream cache log log-directory** command deletes the path for storing logs in NetStream traffic statistics.

By default, the path for storing logs is not configured.

NOTE

Only AR2204E&AR2240&AR2240C, and AR3200 series support the command.

Format

ip netstream cache log log-directory *log-directory*

undo ip netstream cache log log-directory *log-directory*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
log-directory	Indicates the path for storing logs.	The value is a string of 1 to 63 case-insensitive characters without spaces. **NOTE** Logs can be saved to either a USB flash drive or an external SD card, but not the flash directory. The name of the currently used folder and data file in the root directory of the USB flash drive is NetStreamLog/ netstreamdata.db. The logs in NetStream traffic statistics should be stored in the folder using this name. If a folder with the same name exists, the data may fail to be saved or the original file may be overwritten.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **ip netstream cache log log-directory** command to set the path for storing logs in NetStream traffic statistics.

Precautions

If the function of recording logs is enabled globally by running the **ip netstream cache log enable** command, you want to delete the configured path for storing logs in NetStream traffic statistics, you must first run the **undo ip netstream cache log enable** command to disable the function of recording logs globally, and then run the **undo ip netstream cache log log-directory** command.

If the function of recording logs is enabled globally by running the **ip netstream cache log enable** command, you cannot run the **ip netstream cache log log-directory** command to set a new path for storing logs. To change the configured path for storing logs, you need to run the **undo ip netstream cache log enable** command to disable the function of recording logs first.

Copyright © Huawei Technologies Co., Ltd.

Multiple data files can be saved to the fixed folder in the root directory of the USB flash drive, and the size of each data file is 10 MB. For example, if the first data file is netstreamdata.db, the system automatically creates the second data file netstreamdata2.db when the size of the data file exceeds 10 MB. In this manner, the third data file is netstreamdata3.db and the Xth data file is netstreamdatax.db.

Example

Set the path for storing logs in NetStream traffic statistics to usb0.

```
<Huawei> system-view
[Huawei] ip netstream cache log log-directory usb0:
```

Related Topics

21.12.19 ip netstream cache log enable

21.12.21 ip netstream export host

Function

The **ip netstream export host** command configures the destination IP address and destination UDP port number for the exported packets carrying IPv4 flow statistics.

The **undo ip netstream export host** command deletes the configured destination IP address and destination UDP port number for the exported packets carrying IPv4 flow statistics.

By default, no destination IP address and destination UDP port number are configured in the system view or aggregation view for the exported packets carrying IPv4 flow statistics.

Format

ip netstream export host *ip-address port-number* [**vpn-instance** *vpn-instance-name*]

undo ip netstream export host *ip-address port-number* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IPv4 address of the exported packets carrying IPv4 flow statistics.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
port-number	Specifies the destination UDP port number of the exported packets carrying IPv4 flow statistics.	The value is an integer that ranges from 0 to 65535.
vpn-instance *vpn-instance-name*	Specifies the VPN instance of the exported packets carrying IPv4 flow statistics.	The VPN instance has been created on the device.

Views

System view, NetStream aggregation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After finishing data collection, the NDE sends the collected data to the NSC. This command specifies the destination address of the collected data, that is, the NSC IP address.

Precautions

When you run the **ip netstream export host** command in the system view, this command configures the destination address for the exported packets carrying IPv4 original flow statistics and IPv4 flexible flow statistics; when you run this command in the aggregation view, this command configures the destination address for the exported packets carrying IPv4 aggregation flows. The exported packets carrying aggregation flow statistics preferentially use the destination address configured in the aggregation view. If the destination address is not configured in the aggregation view, the exported packets carrying aggregation flow statistics use the destination address configured in the system view.

You can configure two destination addresses in the system view or aggregation view to implement NSC backup. To configure a third destination IP address, run the **undo netstream export ip host** command to delete an existing one first; otherwise, the system displays a message indicating that the maximum number of addresses is exceeded and the configuration fails.

Example

Set the destination IP address for the exported packets carrying original flow statistics to 10.1.1.1, and UDP port number to 222.

```
<Huawei> system-view
[Huawei] ip netstream export host 10.1.1.1 222
```

 Copyright © Huawei Technologies Co., Ltd.

Set the destination IP address for the exported packets carrying aggregation flow statistics to 10.2.2.1, and UDP port number to 255.

```
<Huawei> system-view
[Huawei] ip netstream aggregation as
[Huawei-aggregation-as] ip netstream export host 10.2.2.1 255
```

21.12.22 ip netstream export index-switch

Function

The **ip netstream export index-switch** command sets the number of digits in the interface indexes contained in an exported NetStream packet.

By default, the number of digits in interface indexes is 16.

Format

ip netstream export index-switch *index-switch*

Parameters

Parameter	Description	Value
index-switch	Specifies the number of digits in the index of a specified interface.	The value is 16 or 32. The default value is 16.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **ip netstream export index-switch** command to set the number of digits in the interface index to 16 or 32.

The number of digits in an interface index contained in exported packets must be the same as the number of digits in an interface index that can be parsed by the NMS. For example, if the NMS can parse the 32-digit interface index, set the number of digits in an interface index contained in exported packets to 32.

Precautions

The number of digits in the interface index can be changed to 32 only when the NMS supports 32-digit interface index. If the number of digits in an interface index contained in exported packets is different from the number of digits in an

 Copyright © Huawei Technologies Co., Ltd.

interface index supported by the NMS, the NMS cannot identify NetStream packets sent by the device.

Example

Change the number of digits in the interface index contained in an exported NetStream packet from 16 to 32.

```
<Huawei> system-view
[Huawei] ip netstream export index-switch 32
```

21.12.23 ip netstream export source

Function

The **ip netstream export source** command configures the source address for the exported packets carrying IPv4 flow statistics and source UDP port number.

The **undo ip netstream export source** command restores the default source address and source UDP port number of the exported packets carrying IPv4 flow statistics.

By default, the source IP address of the exported packets carrying IPv4 flow statistics is not configured.

Format

ip netstream export source *ip-address* [*portnumber*]

undo ip netstream export source

Parameters

Parameter	Description	Value
ip-address	Specifies the source IPv4 address of the exported packets carrying IPv4 flow statistics.	-
portnumber	Specifies the source port of the exported packets carrying IPv4 flow statistics.	The value is an integer that ranges from 0 to 65535.

Views

System view, NetStream aggregation view

Default Level

3: Management level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The NMS working with the NetStream system may need to identify the data source based on the source address in NetStream packets. You can run the **ip netstream export source** command to configure the source address of exported packets carrying IPv4 flow statistics.

Precautions

NetStream prefers the source IP and source UDP port number address configured in the aggregation view. If no source address is specified in an aggregation method, the source address configured in the system view is used.

Example

In the system view, set the source address for the exported packets carrying IPv4 flow statistics to 10.1.1.1.

```
<Huawei> system-view
[Huawei] ip netstream export source 10.1.1.1
```

In the aggregation view, set the source address for the exported packets carrying IPv4 flow statistics to 10.2.2.2.

```
<Huawei> system-view
[Huawei] ip netstream aggregation as
[Huawei-aggregation-as] ip netstream export source 10.2.2.2
```

21.12.24 ip netstream export source interface

Function

The **ip netstream export source interface** command configures the outbound interface for the exported packets carrying original flow statistics.

The **undo ip netstream export source** command deletes the outbound interface for the exported packets carrying original flow statistics.

By default, no outbound interface is configured for the exported packets carrying original flow statistics.

Format

ip netstream export source interface *interface-type interface-number* [*port-number*]

undo ip netstream export source

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type	Specifies the type of the outbound interface.	The value can be Ethernet interface, VLANIF interface, dialer interface, and Cellular interface.
interface-number	Specifies the number of the outbound interface.	-
port-number	Specifies the source UDP port of the exported NetStream packet.	The value is an integer that ranges from 0 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The NMS identifies the data source according to the outbound interface in NetStream packets, so you need to run the **ip netstream export source interface** command to set the outbound interface for NetStream packets. When the IP address of the outbound interface changes, NetStream packets can be sent from the outbound interface.

Precautions

The **ip netstream export source interface** command can be used only on Layer 3 interfaces.

Example

Set the outbound interface for the exported packets carrying original flow statistics to GE0/0/1.

```
<Huawei> system-view
[Huawei] ip netstream export source interface gigabitethernet 0/0/1
```

21.12.25 ip netstream export template timeout-rate

Function

The **ip netstream export template timeout-rate** command sets the interval for sending the NetStream export template.

 Copyright © Huawei Technologies Co., Ltd.

The **undo ip netstream export template timeout-rate** command restores the default interval.

By default, the interval for sending the NetStream export template is 30 minutes.

Format

ip netstream export template timeout-rate *timeout-interval*

undo ip netstream export template timeout-rate

Parameters

Parameter	Description	Value
timeout-interval	Specifies the interval for sending the NetStream export template.	The value is an integer in the range from 1 to 3600, in minutes. The default value is 30.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If network traffic is heavy, the template refresh interval should be set to a small value; however, more traffic is generated for sending the template. Therefore, you need to select a proper interval for sending the NetStream export template. In this case, you can run the **ip netstream export template timeout-rate** command to adjust the interval.

Example

Set the interval for sending the NetStream export template to 50 minutes.

```
<Huawei> system-view
[Huawei] ip netstream export template timeout-rate 50
```

21.12.26 ip netstream export version

Function

The **ip netstream export version** command configures the version number of the exported packets carrying original flow statistics.

The **undo ip netstream export version** command restores the default setting.

Copyright © Huawei Technologies Co., Ltd.

By default, the version number of the exported packets carrying IPv4 original flow statistics is 5. Packets of V5 have no AS option and do not carry BGP next hop information.

Format

ip netstream export version *version* [**origin-as** | **peer-as**] [**bgp-nexthop**]

undo ip netstream export version

Parameters

Parameter	Description	Value
version	Specifies the version number of exported packets carrying IPv4 flow statistics.	The value of *version* is set to 5, 9 or 10. The default is 5.
origin-as	Specifies the AS number recorded in the statistics as the original AS number.	-
peer-as	Specifies the AS number recorded in the statistics as the peer AS number.	-
bgp-nexthop	Configures the statistics to carry BGP next hop information. Currently, V9 and V10 support the exported packets carrying BGP next hop information.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The NDE exports NetStream flow statistics to the NSC. The version of exported packets must be the same as that configured on the NSC so that the NSC can parse the exported packets.

 Copyright © Huawei Technologies Co., Ltd.

The format of exported packets in V5 is fixed and is not easy to expand. The format of exported packets in V9 or V10 is defined in templates and is easy to combine or expand. The statistics are exported more flexibly.

Precautions

Only one version can be specified on a device. The versions configured on all the devices on the network must be the same as the version configured on the NMS.

The AS option is used according to the actual situation of the AS configured on each device. The AS option affects only the packet statistics result, but does not affect the flows. The AS option is encapsulated in the AS option field carried in the NetStream packets sent to the NMS. The exported packets of V5 do not support BGP next hop information.

Example

Set the version of the exported packets carrying IPv4 flow statistics to V9 and AS option to **peer-as**.

```
<Huawei> system-view
[Huawei] ip netstream export version 9 peer-as
```

21.12.27 ip netstream multicast

Function

The **ip netstream multicast** command enables the flow statistics collection function for incoming and outgoing IPv4 multicast flows.

The **undo ip netstream multicast** command disables the flow statistics collection function for incoming and outgoing IPv4 multicast flows.

By default, the flow statistics collection function is disabled for incoming and outgoing IPv4 multicast flows.

Format

ip netstream multicast { **inbound** | **outbound** }

undo ip netstream multicast { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Indicates the incoming packets.	-
outbound	Indicates the outgoing packets.	-

Views

Interface view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

The **ip netstream multicast** command allows the device to collect statistics about incoming and outgoing IPv4 multicast packets and export the statistics to the NMS.

Example

Enable the flow statistics collection function for incoming IPv4 multicast packets on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip netstream multicast inbound
```

21.12.28 ip netstream pre-classify enable

Function

The **ip netstream pre-classify enable** command enables the NetStream pre-classify function globally.

The **undo ip netstream pre-classify enable** command disables the NetStream pre-classify function globally.

By default, the pre-classify function is disabled globally.

Format

ip netstream pre-classify enable

undo ip netstream pre-classify enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If you need to collect statistics on original packets when the IPSec, NAT, and VXLAN services are configured together, run the **ip netstream pre-classify enable** command to enable the pre-classify function globally and configure the pre-classify function for original packets.

Copyright © Huawei Technologies Co., Ltd.

The pre-classify function for original packets is configured using the **qos pre-classify** command.

When multiple services are configured, NetStream extracts the template content in the pre-classify configuration order. For example, if VXLAN is configured and then IPSec is configured, and pre-classify is configured for both services, NetStream extracts the original packets from the VXLAN encapsulation first. If pre-classify is configured for only IPSec, NetStream extracts VXLAN encapsulated packets.

Example

Enable NetStream pre-classify globally.

```
<Huawei> system-view
[Huawei] ip netstream pre-classify enable
```

21.12.29 ip netstream record

Function

The **ip netstream record** command creates a new flexible flow statistics template or displays the view of an existing flexible statistics template.

The **undo ip netstream record** command deletes a specified flexible flow statistics template.

By default, no flexible flow statistics template exists.

Format

ip netstream record *record-name*

undo ip netstream record *record-name*

Parameters

Parameter	Description	Value
record-name	Specifies the name of the flexible flow statistics template.	The value is a string of 1 to 20 case-sensitive characters without spaces. The name of the flexible flow statistics template cannot contain special characters such as @, %, or *.

Views

System view

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You need to create the flexible flow statistics template before exporting flexible flow statistics.

Precautions

A maximum of 16 flexible flow statistics templates can be configured on one device. To configure a third flexible flow statistics template, run the **undo ip netstream record** command to delete an existing one first.

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. To delete this flexible flow statistics template, run the **undo port ip netstream record** command on the interface and then modify or delete the template.

Example

Create the flexible flow statistics template named **abc**.

```
<Huawei> system-view
[Huawei] ip netstream record abc
[Huawei-record-abc]
```

Related Topics

21.12.41 port ip netstream record

21.12.7 display ip netstream record

21.12.30 ip netstream rpf-failure

Function

The **ip netstream rpf-failure** command enables NetStream functions for collecting statistics about flows that fail the RPF check.

The **undo ip netstream rpf-failure** command disables NetStream functions from collecting statistics about flows that fail the RPF check.

By default, NetStream functions are disabled from collecting statistics about flows that fail the RPF check.

Format

ip netstream rpf-failure inbound

undo ip netstream rpf-failure inbound

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

3: Management level

Usage Guidelines

You need to enable the RPF check before configuring NetStream functions for collecting statistics about flows that fail the RPF check.

Example

Enable RPF statistics function on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip netstream rpf-failure inbound
```

21.12.31 ip netstream sampler (interface view)

Function

The **ip netstream sampler** command configures the packet sampling function for IPv4 packets on an interface.

The **undo ip netstream sampler** command restores the default setting.

By default, the packet-based regular sampling is used. The default packet sampling ratio is 100.

Format

ip netstream sampler { **fix-packets** *packet-interval* | **fix-time** *time-interval* | **random-packets** *packet-interval* | **random-time** *time-interval* } { **inbound** | **outbound** }

undo ip netstream sampler { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
fix-packets *packet-interval*	Indicates the number of packets between two sampled packets in the packet-based regular sampling.	The value is an integer that ranges from 1 to 65535.
fix-time *time-interval*	Indicates the interval of time-based regular sampling.	The value is an integer that ranges from 5 to 30000, in milliseconds.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
random-packets *packet-interval*	Indicates the number of packets between two sampled packets in the packet-based random sampling.	The value is an integer that ranges from 1 to 65535.
random-time *time-interval*	Indicates the interval of time-based random sampling.	The value can be the following: • 3.0 • 6.0 • 12.0 • 24.0 • 48.0 • 96.0 • 192.0 • 383.5 • 767.0 • 1534.0 • 3068.0 • 6136.0 The unit is millisecond.
inbound	Samples incoming traffic on an interface.	-
outbound	Samples outgoing traffic on an interface.	-

Views

Interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can set an interval for sampling packets so that only statistics about sampled packets are collected. The statistics show the flow status on the entire network. The sampling function reduces NetStream impact on device performance.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

You must run the **ip netstream sampler** command together with the **21.12.13 ip netstream** command. If you run only the **ip netstream sampler** command, the command does not take effect.

If you run the **ip netstream sampler** command multiple times in the same view, only the latest configuration takes effect.

Example

Set the packet-based regular sampling ratio for the incoming packets on Eth2/0/0 to 1200.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip netstream sampler fix-packets 1200 inbound
[Huawei-Ethernet2/0/0] ip netstream inbound
```

Related Topics

21.12.13 ip netstream

21.12.32 ip netstream tcp-flag enable

Function

The **ip netstream tcp-flag enable** command configures the aging of NetStream traffic according to the FIN flag or the RST flag in the TCP packet header.

The **undo ip netstream tcp-flag enable** command restores the default setting.

By default, NetStream flows are not aged according to the FIN or RST flag in the TCP packet header.

Format

ip netstream tcp-flag enable

undo ip netstream tcp-flag enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Copyright © Huawei Technologies Co., Ltd.

The FIN or RST flag in a TCP packet indicates that the TCP connection is terminated. When receiving a packet with the FIN or RST flag, the device immediately ages the corresponding NetStream flow. If the **ip netstream tcp-flag enable** command is not run, NetStream flows are aged by following other criteria, for example, inactive aging time or bytes overflow.

Precautions

If you set multiple aging modes on the device, a flow is aged when it matches any criterion.

Only original flows can be aged according to the FIN or RST flag in the TCP packet header.

Example

Configure the aging of original flows according to the FIN or RST flag in the TCP packet header.

```
<Huawei> system-view
[Huawei] ip netstream tcp-flag enable
```

21.12.33 ip netstream tm-after enable

Function

The **ip netstream tm-after enable** command enables the NetStream sampling function after queue scheduling.

The **undo ip netstream tm-after enable** command restores the default setting.

By default, NetStream sampling is performed before queue scheduling.

Format

ip netstream tm-after enable

undo ip netstream tm-after enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

By default, NetStream sampling is performed before queue scheduling. If a local device discards packets, the bandwidth calculated based on sampling data is greater than the bandwidth configured on the interface. To resolve this problem, run the **ip netstream tm-after enable** command to enable the NetStream sampling function after queue scheduling.

Example

Enable the NetStream sampling function after queue scheduling.

```
<Huawei> system-view
[Huawei] ip netstream tm-after enable
```

21.12.34 ip netstream timeout active

Function

The **ip netstream timeout active** command configures the active flow aging time.

The **undo ip netstream timeout active** command restores the default setting.

By default, the active flow aging time is 30 minutes.

Format

ip netstream timeout active *active-interval*

undo ip netstream timeout active

Parameters

Parameter	Description	Value
active-interval	Specifies the active aging time.	The value is an integer that ranges from 1 to 60, in minutes. The default is 30.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Network traffic may burst intermittently, while the memory capacity of the NDE is limited. Earlier flows in the memory need to be exported to release space for the new flows. The process of exporting old flows is called aging. All flows in the NDE memory will be exported to the NSC for analysis.

Copyright © Huawei Technologies Co., Ltd.

When the active time (from flow creation time to the current time) of a flow exceeds the specified active aging time, the flow is exported to the destination.

To quickly detect the status of an active flow, set the active time to a small value; however, this setting increases the frequency at which NetStream packets are sent. To reduce the frequency at which NetStream packets are exported and improve statistics collecting efficiency, set the active time to a large value.

Precautions

If you set multiple aging modes on the device, a flow is aged when it matches any criterion.

Example

Set the active aging time to 20 minutes.

```
<Huawei> system-view
[Huawei] ip netstream timeout active 20
```

21.12.35 ip netstream timeout inactive

Function

The **ip netstream timeout inactive** command configures the inactive aging time.

The **undo ip netstream timeout inactive** command restores the default setting.

By default, the inactive aging time is 30 seconds.

Format

ip netstream timeout inactive *inactive-interval*

undo ip netstream timeout inactive

Parameters

Parameter	Description	Value
inactive-interval	Specifies the inactive aging time.	The value is an integer that ranges from 10 to 600, in seconds. The default is 30.

Views

System view

Default Level

3: Management level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Network traffic may burst intermittently, while the memory capacity of the NDE is limited. Earlier flows in the memory need to be exported to release space for the new flows. The process of exporting old flows is called aging. All flows in the NDE memory will be exported to the NSC for analysis.

When the inactive time (from the last packet receiving time to the current time) of an original or flexible flow exceeds the specified inactive aging time, the flow is exported to the destination.

To quickly detect the status of an inactive flow, set the inactive time to a small value; however, this setting increases the frequency at which NetStream packets are sent. To reduce the frequency at which NetStream packets are exported and improve statistics collecting efficiency, set the inactive time to a large value.

Precautions

If you set multiple aging modes on the device, a flow is aged when it matches any criterion.

Example

Set the inactive aging time to 20 seconds.

```
<Huawei> system-view
[Huawei] ip netstream timeout inactive 20
```

21.12.36 ip-mpls netstream

Function

The **ip-mpls netstream** command enables the function of collecting statistics about IPv4 and MPLS flows in the inbound and outbound directions of an interface.

The **undo ip-mpls netstream** command restores the default configuration.

By default, the function of collecting statistics about IPv4 and MPLS flows in the inbound and outbound directions of an interface is disabled.

NOTE

This command is supported only by the AR1200, AR2200, AR3200, and AR3600 series routers.

Format

ip-mpls netstream { **inbound** | **outbound** }

undo ip-mpls netstream { **inbound** | **outbound** }

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
inbound	Enables the function of collecting statistics about IPv4 and MPLS flows in the inbound direction of an interface.	-
outbound	Enables the function of collecting statistics about IPv4 and MPLS flows in the outbound direction of an interface.	-

Views

Ethernet interface view, Ethernet sub-interface view, GigabitEthernet interface view, GigabitEthernet sub-interface view, XGigabitEthernet interface view, XGigabitEthernet sub-interface view, serial interface view, or serial sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

In the NetStream implementation, you must run this command to enable the flow statistics collection function on an interface so that the statistics about IPv4 and MPLS flows can be displayed.

Precautions

The **ip netstream**, **mpls netstream**, and **ip-mpls netstream** commands are mutually exclusive. Only one of these commands can be enabled on an interface.

If NetStream is configured on a main interface but the sampling ratio is not configured using the **21.12.31 ip netstream sampler (interface view)** command, the main interface samples packets based on the fixed sampling ratio of 1/100. Otherwise, the main interface samples packets based on the configured sampling ratio.

If the **port ip netstream record** command is configured on an interface, the **ip-mpls netstream** command cannot be configured.

When the **ip-mpls netstream** command is run and the version of the exported packets is 9, the device sends the original flow template with ID 1317 to the server.

Copyright © Huawei Technologies Co., Ltd.

MPLS traffic in MPLS over GRE and L2VPN scenarios is not supported. Statistics about aggregation flows and flexible flows of MPLS traffic cannot be collected. MPLS traffic statistics collection based on MQC is not supported.

Example

Enable the function of collecting statistics about IPv4 and MPLS flows in the inbound direction of Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip-mpls netstream inbound
```

Related Topics

21.12.31 ip netstream sampler (interface view)

21.12.37 mpls netstream

Function

The **mpls netstream** command enables the function of collecting statistics about MPLS flows in the inbound and outbound directions of an interface.

The **undo mpls netstream** command restores the default configuration.

By default, the function of collecting statistics about MPLS flows in the inbound and outbound directions of an interface is disabled.

NOTE

This command is supported only by the AR1200, AR2200, AR3200, and AR3600 series routers.

Format

mpls netstream { **inbound** | **outbound** }

undo mpls netstream { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Enables the function of collecting statistics about MPLS flows in the inbound direction of an interface.	-
outbound	Enables the function of collecting statistics about MPLS flows in the outbound direction of an interface.	-

Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, Ethernet sub-interface view, GigabitEthernet interface view, GigabitEthernet sub-interface view, XGigabitEthernet interface view, XGigabitEthernet sub-interface view, serial interface view, or serial sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

In the NetStream implementation, you must run this command to enable the flow statistics collection function on an interface so that the statistics about MPLS flows can be displayed.

Precautions

The **ip netstream**, **mpls netstream**, and **ip-mpls netstream** commands are mutually exclusive. Only one of these commands can be enabled on an interface.

If NetStream is configured on a main interface but the sampling ratio is not configured using the **21.12.31 ip netstream sampler (interface view)** command, the main interface samples packets based on the fixed sampling ratio of 1/100. Otherwise, the main interface samples packets based on the configured sampling ratio.

If the **port ip netstream record** command is configured on an interface, the **mpls netstream** command cannot be configured.

When the **mpls netstream** command is run and the version of the exported packets is 9, the device sends the original flow template with ID 1317 to the server.

MPLS traffic in MPLS over GRE and L2VPN scenarios is not supported. Statistics about aggregation flows and flexible flows of MPLS traffic cannot be collected. MPLS traffic statistics collection based on MQC is not supported.

Example

Enable the function of collecting statistics about MPLS flows in the inbound direction of Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] mpls netstream inbound
```

Related Topics

21.12.31 ip netstream sampler (interface view)

21.12.38 mask

Copyright © Huawei Technologies Co., Ltd.

Function

The **mask** command sets the aggregation mask length.

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

By default, no aggregation mask is configured.

Format

mask { **source** | **destination** } **minimum** *mask-length*

undo mask { **source** | **destination** }

Parameters

Parameter	Description	Value
source	Indicates the aggregation mask of the source address. It is used in the following aggregation methods: prefix, prefix-ToS, source-prefix, and source-prefix-ToS.	-
destination	Indicates the aggregation mask of the destination address. It is used in the following aggregation methods: prefix, prefix-ToS, destination-prefix, or destination-prefix-ToS.	-
mask-length	Specifies the aggregation mask length.	The value is an integer that ranges from 1 to 32.

Views

NetStream aggregation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system uses the larger value between the set mask and the largest mask in the FIB table. If the aggregation mask is not configured, the system uses the mask in the FIB table for aggregation.

Precaution

Aggregation masks are applied to six aggregation methods: **destination-prefix**, **destination-prefix-tos**, **prefix**, **prefix-tos**, **source-prefix**, and **source-prefix-tos**.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the aggregation mask length in the source-prefix aggregation method to 24.

```
<Huawei> system-view
[Huawei] ip netstream aggregation source-prefix
[Huawei-aggregation-srcpre] mask source minimum 24
```

21.12.39 match ipv4

Function

The **match ipv4** command configures aggregation keywords in an IPv4 flexible flow statistics template.

The **undo match ipv4** command deletes aggregation keywords from an IPv4 flexible flow statistics template.

Format

match ipv4 { **protocol** | **tos** | **source-address** | **destination-address** | **source-port** | **destination-port** }

undo match ipv4 { **protocol** | **tos** | **source-address** | **destination-address** | **source-port** | **destination-port** }

Parameters

Parameter	Description	Value
protocol	Indicates the IP protocol aggregation.	-
tos	Indicates the ToS priority aggregation.	-
source-address	Indicates the source IP address aggregation.	-
destination-address	Indicates the destination IP address aggregation.	-
source-port	Indicates the source port number aggregation.	-
destination-port	Indicates the destination port aggregation.	-

Views

Flexible flow statistics template view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You need to create a flexible flow statistics template using the **21.12.29 ip netstream record** command before running the **match ipv4** command.

When you run the **match ipv4** command to configure the aggregation keywords, only one keyword can be configured each time. If you run this command multiple times in the same view, a set of multiple aggregation keywords is configured. If a template has been applied to an interface, you cannot modify or delete aggregation keywords from the template.

Example

Set the flexible flow statistics template **abc1** to aggregate flows based on the source port number.

```
<Huawei> system-view
[Huawei] ip netstream record abc1
[Huawei-record-abc1] match ipv4 source-port
```

Related Topics

21.12.29 ip netstream record

21.12.40 match vxlan vni

Function

The **match vxlan vni** command configures the VXLAN VNI aggregation keyword for record.

The **undo match vxlan vni** command deletes the VXLAN VNI aggregation keyword.

By default, no VXLAN VNI aggregation keyword is configured in a flexible flow statistics template.

Format

match vxlan vni

undo match vxlan vni

Parameters

None

Views

Flexible flow template view

Default Level

3: Management level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The VXLAN Network Identifier (VNI) is similar to a VLAN ID. It is used to divide VXLAN segments. When you configure VNI in the flexible flow statistics template, run this command to set the aggregation keyword.

Prerequisites

A flexible flow statistics template has been created or the flexible flow statistics template view is displayed using the **ip netstream record** command.

Precautions

When you run the **match vxlan vni** command to configure the VXLAN VNI aggregation keyword for record, if the record view has been applied to an interface, the aggregation keyword cannot be modified or deleted.

Only a VXLAN-capable device supports this command.

NOTE

Only the AR100, AR120, AR150, AR160, AR200, AR1200 series, AR2220E, AR2240, and AR3260 support VXLAN. AR2220E, AR2240, and AR3260 need to run the **portswitch** command to change the working mode of all interfaces on the SRU200, SRU400, 4GECS, and 2X10GL from Layer 3 mode to Layer 2 mode. The interfaces that change the working mode to layer 2 only support VXLAN. Only the 8FE1GE, 24GE, and 24ES2GP ethernet LAN card support VXLAN.

Only the AR100, AR120, AR150, AR160 (except AR161EW, AR161EW-M1, AR169EW, AR169EGW-L), AR200, AR1200series, AR2220E support EVPN.

Example

Configure the **abc1** record to aggregate flows based on the VNI type.

```
<Huawei> system-view
[Huawei] ip netstream record abc1
[Huawei-record-abc1] match vxlan vni
```

Related Topics

21.12.29 ip netstream record

21.12.41 port ip netstream record

Function

The **port ip netstream record** command applies the flexible flow statistics template to an interface.

The **undo port ip netstream record** command deletes a specified flexible flow statistics template on an interface.

By default, no flexible flow statistics template is applied to an interface.

Format

port ip netstream record *record-name*

Copyright © Huawei Technologies Co., Ltd.

undo port ip netstream record

Parameters

Parameter	Description	Value
record-name	Specifies the name of a flexible flow statistics template.	The value is a string of 1 to 20 case-sensitive characters without spaces. The name of the flexible flow statistics template cannot contain special characters such as \, /, :, <, >, |, @, ', % or *. The value is the same as the IPv4 flexible flow statistics template name configured using the **ip netstream record** command.

Views

Interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a flexible flow statistics template is configured, run the **port ip netstream record** command to apply the template to an interface.

The interface then aggregates flows based on the configured aggregation keywords, collects flow statistics, and exports aged flows to the NSC.

Prerequisites

The flexible flow statistics template has been created and at least one aggregation keyword has been configured using the **match ip4** command.

Precautions

Each interface can be configured with only one flexible flow statistics template. Before modifying the flexible flow statistics template in the same interface view, run the **undo port ip netstream record** command to delete the existing configuration.

If the flexible flow statistics template has been applied to an interface, the template configuration cannot be modified or deleted.

 Copyright © Huawei Technologies Co., Ltd.

When flow statistics collection is enabled both on the inbound and outbound interfaces, the **port ip netstream record** command does not take effect.

Example

Configure the flexible flow statistics template **abc1** (aggregating flows based on the source and destination IP addresses, collecting statistics about the number of packets, and exporting the inbound interface index). Apply such configurations to Eth2/0/0.

```
<Huawei> system-view
[Huawei] ip netstream record abc1
[Huawei-record-abc1] match ipv4 source-address
[Huawei-record-abc1] match ipv4 destination-address
[Huawei-record-abc1] collect counter packets
[Huawei-record-abc1] collect interface input
[Huawei-record-abc1] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port ip netstream record abc1
 Info: Interface got a record config succeed.
```

Related Topics

21.12.29 ip netstream record

21.12.13 ip netstream

21.12.42 reset ip netstream cache

Function

The **reset ip netstream cache** command forcibly ages all the flows in the cache.

Format

reset ip netstream cache

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Forced aging is used when you require the latest statistics, but you do not satisfy with the existing aging conditions or some flows fail to age out due to an anomaly. You can forcibly age out all the original flows in the cache and export the flow statistics.

Copyright © Huawei Technologies Co., Ltd.

Example

Age all the flows in the cache forcibly.

```
<Huawei> system-view
[Huawei] reset ip netstream cache
```

21.12.43 reset ip netstream statistic

Function

The **reset ip netstream statistic** command deletes NetStream flow statistics.

Format

reset ip netstream statistic

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When diagnosing and locating network faults, collect flow statistics in a specified period. Before statistics collection starts, you can run this command to delete historical statistics.

Precautions

The **reset ip netstream statistic** command deletes all NetStream statistics. The statistics cannot be restored after being deleted. Therefore, confirm the action before running this command.

You can run this command multiple times at any interval.

Example

Delete NetStream statistics.

```
<Huawei> reset ip netstream statistic
```


Copyright © Huawei Technologies Co., Ltd.

21.12.44 snmp-agent trap enable feature-name netstream

Function

The **snmp-agent trap enable feature-name netstream** command enables the NetStream trap function on the device.

The **undo snmp-agent trap enable feature-name netstream** command disables the NetStream trap function on the device.

By default, the NetStream trap function is disabled.

Format

snmp-agent trap enable feature-name netstream [**trap-name hwnetstreamsessionfull**]

undo snmp-agent trap enable feature-name netstream [**trap-name hwnetstreamsessionfull**]

Parameters

Parameter	Description	Value
trap-name	Specifies the name of the trap for a specified event.	-
hwnetstreamsessionfull	Sends Huawei-proprietary trap messages when the NetStream session table is full.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

None

Example

Enable the NetStream trap function on the device.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name netstream
```

 Copyright © Huawei Technologies Co., Ltd.

21.12.45 snmp-agent trap enable feature-name sindex

Function

The **snmp-agent trap enable feature-name sindex** command enables the trap function for the SINDEX module.

The **undo snmp-agent trap enable feature-name sindex** command disables the trap function for the SINDEX module.

By default, the trap function is enabled for the SINDEX module.

Format

snmp-agent trap enable feature-name sindex [**trap-name hwnetstreamindexusedup**]

undo snmp-agent trap enable feature-name sindex [**trap-name hwnetstreamindexusedup**]

Parameters

Parameter	Description	Value
trap-name	Specifies the name of the trap for a specified event on the SINDEX module.	-
hwnetstreamindexusedup	Sends Huawei-proprietary trap messages when all interface indexes are allocated.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

None

Example

Enable the trap function for the SINDEX module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name sindex
```

 Copyright © Huawei Technologies Co., Ltd.

21.13 IP Accounting Configuration Commands

21.13.1 display ip accounting input-packets

Function

The **display ip accounting input-packets** command displays statistics about incoming IP packets.

Format

display ip accounting input-packets { **matched** | **mismatched** } [**top**]

Parameters

Parameter	Description	Value
matched	Displays incoming packet statistics records in the matched table. **NOTE** The matched table stores statistics about the packets matching the IP accounting rules.	-
mismatched	Displays incoming packet statistics records in the mismatched table. **NOTE** The mismatched table stores: • Statistics about the packets not matching the IP accounting rules. • Common IP accounting statistics if no IP accounting rule is configured.	-
top	Displays the top 32 records with the most packets in a statistics table. If the table contains less than 32 records, all records will be displayed. **NOTE** If the **top** parameter is not specified, all records in the table are displayed.	-

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Background

The **display ip accounting input-packets** command displays statistics about incoming IP packets. These statistics help you monitor network traffic.

Precautions

The default upper threshold of the mismatched table is 0. To store records into the mismatched table, change the upper threshold; otherwise, no information is displayed for the mismatched table.

Example

Display incoming packet statistics in the matched table.

```
<Huawei> display ip accounting input-packets matched
The matched list contains 2 incoming streams.
Source          Destination     Protocol Packets     Bytes       Age(Unit:Min)
10.138.78.120   192.168.200.155 6        104          4821        0
10.138.78.119   192.168.200.155 6        17           782         0
```

Table 21-75 Description of the display ip accounting input-packets command output

Item	Description
Source	Source address of IP packets.
Destination	Destination addresses of IP packets.
Protocol	Packet protocol.
Packets	Number of packets.
Bytes	Number of bytes.
Age(Unit:Min)	Update time of date flows, in minutes.

Related Topics

21.13.2 display ip accounting output-packets

21.13.3 display ip accounting precedence

21.13.5 ip accounting

Copyright © Huawei Technologies Co., Ltd.

21.13.2 display ip accounting output-packets

Function

The **display ip accounting output-packets** command displays statistics about outgoing IP packets.

Format

display ip accounting output-packets { **matched** | **mismatched** } [**top**]

Parameters

Parameter	Description	Value
matched	Displays outgoing packet statistics records in the matched table. **NOTE** The matched table stores statistics about the packets matching the IP accounting rules.	-
mismatched	Displays outgoing packet statistics records in the mismatched table. **NOTE** The mismatched table stores: • Statistics about the packets not matching the IP accounting rules. • Common IP accounting statistics if no IP accounting rule is configured.	-
top	Displays the top 32 records with the most packets in a statistics table. If the table contains less than 32 records, all records will be displayed. **NOTE** If the **top** parameter is not specified, all records in the table are displayed.	-

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Background

The **display ip accounting output-packets** command displays statistics about outgoing IP packets. These statistics help you monitor network traffic.

Precautions

The default upper threshold of the mismatched table is 0. To store records into the mismatched table, change the upper threshold; otherwise, no information is displayed for the mismatched table.

Example

Display outgoing packet statistics in the matched table.

```
<Huawei> display ip accounting output-packets matched
The matched list contains 1 outgoing streams.
Source          Destination     Protocol Packets     Bytes       Age(Unit:Min)
192.168.1.112   192.168.1.255   17       5           1145        2
```

Table 21-76 Description of the display ip accounting output-packets command output

Item	Description
Source	Source address of IP packets.
Destination	Destination addresses of IP packets.
Protocol	Packet protocol.
Packets	Number of packets.
Bytes	Number of bytes.
Age(Unit:Min)	Update time of date flows, in minutes.

Related Topics

21.13.1 display ip accounting input-packets

21.13.3 display ip accounting precedence

21.13.5 ip accounting

21.13.3 display ip accounting precedence

Function

The **display ip accounting precedence** command displays statistics about IP precedence accounting.

Copyright © Huawei Technologies Co., Ltd.

Format

display ip accounting precedence

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Precautions

The statistics about IP precedence accounting are stored in a dedicated statistics table.

Example

Display statistics about IP precedence accounting.

```
<Huawei> display ip accounting precedence
Precedence Packets         Bytes
Input
0          11920           1480947
Output
0          200             32889
```

Table 21-77 Description of the display ip accounting precedence command output

Item	Description
Precedence	IP packet precedence, ranging from 0 to 7.
Packets	Number of packets.
Bytes	Number of bytes.
Input	Statistics about incoming packets.
Output	Statistics about outgoing packets.

Related Topics

21.13.1 display ip accounting input-packets

21.13.2 display ip accounting output-packets

21.13.8 ip accounting precedence

Copyright © Huawei Technologies Co., Ltd.

21.13.4 display ip accounting rule

Function

The **display ip accounting rule** command displays IP accounting rules.

Format

display ip accounting rule

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Background

The **display ip accounting rule** command displays all configured IP accounting rules for you to manage the rules.

Example

Display IP accounting rules.

```
<Huawei> display ip accounting rule
 IP Accounting rule list:
 IP address:             address mask:
 192.168.0.1              255.255.255.255
 192.168.0.2              255.255.255.255
 ----------------------------------------
 Total: 2 rules
```

Table 21-78 Description of the display ip accounting rule command output

Item	Description
IP address	IP address in an IP accounting rule.
address mask	Subnet mask in an IP accounting rule.

Related Topics

21.13.9 ip accounting rule

Copyright © Huawei Technologies Co., Ltd.

21.13.5 ip accounting

Function

The **ip accounting** command enables IP accounting for the incoming or outgoing packets on an interface.

The **undo ip accounting** command disables IP accounting on an interface.

By default, IP accounting is disabled on all interfaces.

Format

ip accounting { **input-packets** | **output-packets** }

undo ip accounting { **input-packets** | **output-packets** }

Parameters

Parameter	Description	Value
input-packets	Enables IP accounting for the incoming packets on an interface.	-
output-packets	Enables IP accounting for the outgoing packets on an interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect statistics on the incoming or outgoing packets on an interface, run the **ip accounting** command to enable IP accounting on the interface.

Example

Enable IP accounting for the incoming packets on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip accounting input-packets
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.13.1 display ip accounting input-packets

21.13.2 display ip accounting output-packets

21.13.6 ip accounting matched-threshold

Function

The **ip accounting matched-threshold** command sets the upper threshold for a matched table.

The **undo ip accounting matched-threshold** command restores the default upper threshold of a matched table.

By default, the upper threshold of a matched table is 512.

Format

ip accounting matched-threshold *thresh-value*

undo ip accounting matched-threshold

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
thresh-value	Indicates the upper threshold of a matched table.	The value is an integer and the value range differs in various product series. On the AR100&AR120&AR150&AR160&200 series, the value ranges from 0 to 1024. On the AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, and AR2204, the value ranges from 0 to 4096. On the AR2220L, AR2220E, AR2240C, AR2220, and AR2240, the value ranges from 0 to 8192. On the AR3200&AR3600 series, the value ranges from 0 to 16384. The default value is 512.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A matched table stores statistics about the packets matching the IP accounting rules. The **ip accounting matched-threshold** command specifies the maximum number of records stored in the matched table. When the number of stored records reaches the upper threshold, new records cannot be added to the matched table.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The matched table does not store the statistics records of IP precedence accounting.

Example

Set the upper threshold for a matched table to 1000.

```
<Huawei> system-view
[Huawei] ip accounting matched-threshold 1000
```

Related Topics

21.13.7 ip accounting mismatched-threshold

21.13.7 ip accounting mismatched-threshold

Function

The **ip accounting mismatched-threshold** command sets the upper threshold for a mismatched table.

The **undo ip accounting mismatched-threshold** command restores the default upper threshold of a mismatched table.

By default, the upper threshold of a mismatched table is 0.

Format

ip accounting mismatched-threshold *thresh-value*

undo ip accounting mismatched-threshold

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
thresh-value	Indicates the upper threshold of a mismatched table.	The value is an integer and the value range differs in various product series. On the AR100&AR120&AR150&160&200 series, the value ranges from 0 to 1024. On the AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, and AR2204, the value ranges from 0 to 4096. On the AR2220L, AR2220E, AR2240C, AR2220, and AR2240, the value ranges from 0 to 8192. On the AR3200&AR3600 series, the value ranges from 0 to 16384. The default value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When common IP accounting is enabled without IP accounting rules configured, all statistics are recorded in the mismatched table. When common IP accounting is enabled with IP accounting rules configured, statistics about the packets that do not match the IP accounting rules are recorded in the mismatched table. The **ip accounting mismatched-threshold** command specifies the maximum number of records stored in the mismatched table. When the number of stored records reaches the upper threshold, new records cannot be added to the mismatched table.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The default upper threshold of a mismatched table is 0. To store records into the mismatched table, change the upper threshold; otherwise, the mismatched table does not store records.

The mismatched table does not store the statistics records of IP precedence accounting.

Example

Set the upper threshold for a mismatched table to 1000.

```
<Huawei> system-view
[Huawei] ip accounting mismatched-threshold 1000
```

Related Topics

21.13.6 ip accounting matched-threshold

21.13.8 ip accounting precedence

Function

The **ip accounting precedence** command enables IP precedence accounting for the incoming or outgoing packets on an interface.

The **undo ip accounting precedence** command disables IP precedence accounting for the incoming or outgoing packets on an interface.

By default, IP precedence accounting is disabled on interfaces.

Format

ip accounting precedence { **input-packets** | **output-packets** }

undo ip accounting precedence { **input-packets** | **output-packets** }

Parameters

Parameter	Description	Value
input-packets	Enables IP precedence accounting for the incoming packets on an interface.	-
output-packets	Enables IP precedence accounting for the outgoing packets on an interface.	-

Views

Interface view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IP precedence ranges from 0 to 7. The **ip accounting precedence** command collects statistics about the packets with each IP precedence.

Prerequisite

The **ip accounting** { **input-packets** | **output-packets** } command has been executed to enable common IP accounting for the incoming or outgoing packets on the interface.

NOTE

For example, to use IP precedence accounting on the packets received by an interface, first enable common IP accounting for the incoming packets on the interface. The directions to which common IP accounting and IP precedence accounting apply must be the same.

Example

Enable IP precedence accounting for the incoming packets on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip accounting input-packets
[Huawei-GigabitEthernet1/0/0] ip accounting precedence input-packets
```

Related Topics

21.13.3 display ip accounting precedence

21.13.9 ip accounting rule

Function

The **ip accounting rule** command creates IP accounting rules.

The **undo ip accounting rule** command deletes IP accounting rules.

By default, no IP accounting rule is configured.

Format

ip accounting rule *ip-address* { *mask* | *mask-length* }

undo ip accounting rule [*ip-address* { *mask* | *mask-length* }]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Indicates the IP address in an IP accounting rule.	The value is in dotted decimal notation.
mask	Indicates the subnet mask in an IP accounting rule.	The value is in dotted decimal notation.
mask-length	Indicates the mask length.	The value is an integer that ranges from 0 to 32.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **ip accounting rule** command is executed, statistics about the packets with source or destination addresses matching the IP accounting rule are recorded in the matched table. Statistics about the packets not matching the IP accounting rule are recorded in the mismatched table.

Precautions

IP accounting contains a maximum of 32 rules. When an IP packet matches any IP accounting rule, statistics about the packet are recorded in the matched table.

NOTE

IP precedence accounting does not have rules.

Example

Collect statistics about the packets with source or destination address 192.168.0.1/32.

```
<Huawei> system-view
[Huawei] ip accounting rule 192.168.0.1 255.255.255.255
```

Related Topics

21.13.4 display ip accounting rule

 Copyright © Huawei Technologies Co., Ltd.

21.13.10 ip accounting timeout

Function

The **ip accounting timeout** command sets the aging time for IP accounting statistics records.

The **undo ip accounting timeout** command restores the default aging time of IP accounting statistics records.

By default, the aging time of IP accounting statistics records is 720 minutes (12 hours).

Format

ip accounting timeout *time-value*

undo ip accounting timeout

Parameters

Parameter	Description	Value
time-value	Indicates the aging time of IP accounting statistics records.	The value is an integer that ranges from 60 to 10080, in minutes. The default value is 720.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a statistics record is not updated within the aging time, the record is aged out and deleted.

Precautions

The aging time does not apply to IP precedence accounting. The records in the statistics table of IP precedence accounting can only be deleted manually using the **reset ip accounting precedence** command.

Example

Set the aging time of IP accounting statistics records to 60 minutes.

Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ip accounting timeout 60
```

21.13.11 reset ip accounting

Function

The **reset ip accounting** command clears IP accounting statistics.

Format

reset ip accounting { **all** | **matched** | **mismatched** | **precedence** }

Parameters

Parameter	Description	Value
all	Clears all statistics tables.	-
matched	Clears the matched table. **NOTE** The matched table stores statistics about the packets matching the IP accounting rules.	-
mismatched	Clears the mismatched table. **NOTE** The mismatched table stores: • Statistics about the packets not matching the IP accounting rules. • Common IP accounting statistics if no IP accounting rule is configured.	-
precedence	Clears the statistics table of IP precedence accounting. **NOTE** This table stores the statistics records of IP precedence accounting.	-

Views

User view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Precautions

Before collecting packet statistics, you should clear existing statistics records; otherwise, statistics are inaccurate. If you do not clear them, the records will not be deleted until the aging time expires.

Example

Clear all statistics tables.

```
<Huawei> reset ip accounting all
```

Related Topics

21.13.1 display ip accounting input-packets

21.13.2 display ip accounting output-packets

21.14 TWAMP Light Configuration Commands

NOTE

AR3670 do not support TWAMP Light.

21.14.1 client

Function

The **client** command enables the TWAMP Light Client function and displays the Client view. If the Client function has been enabled, this command directly displays the Client view.

The **undo client** command disables the TWAMP Light Client function.

By default, the TWAMP Light Client function is disabled.

Format

client

undo client

Parameters

None

Views

TWAMP-Light view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use the TWAMP Light service, run the **client** command to display the Client view and create a TWAMP Light session. The measurement service is started based on the session configuration.

Precautions

When the TWAMP Light Client function is disabled, all TWAMP Light sessions are deleted and the measurement service is stopped.

Example

Enable the TWAMP Light Client function.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] client
[Huawei-twamp-light-client]
```

21.14.2 display twamp-light responder test-session

Function

The **display twamp-light responder test-session** command displays real-time measurement session information on the TWAMP Light reflector.

Format

display twamp-light responder test-session [**verbose** | *session-id*]

Parameters

Parameter	Description	Value
verbose	Displays details about a measurement session on the TWAMP Light reflector.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
session-id	Displays real-time information about the specified measurement session on the TWAMP Light reflector.	The value is an integer. • For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. • For AR1200 series, the value ranges from 1 to 128. • For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. • For AR2240C, the value ranges from 1 to 256. • AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. • For AR3600 series, the value ranges from 1 to 1024.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the continual or on-demand performance measurement function is enabled, you can run this command to view real-time measurement session information on the TWAMP Light reflector if you want to check the measurement session configuration or locate the fault in measurement.

Example

Display the summary of all measurement sessions.

```
<Huawei> display twamp-light responder test-session
Total number : 5
------------------------------------------------------------------------------
  ID    Local-IP       Local-Port    Remote-IP      Remote-Port
------------------------------------------------------------------------------
   2    192.168.1.1         10000    192.168.1.6          20000
   3    192.168.1.2         10000    192.168.1.6          20000
   4    192.168.1.3         10000    192.168.1.6          20000
   5    192.168.1.4         10000    192.168.1.6          20000
   6    192.168.1.5         10000    192.168.1.6          20000
```


Copyright © Huawei Technologies Co., Ltd.

Table 21-79 Description of the **display twamp-light responder test-session** command output

Item	Description
Total number	Total number of sessions.
ID	Measurement session ID.
Local-IP	IP address of the session reflector.
Local-Port	UDP port number of the session reflector.
Remote-IP	IP address of the session sender.
Remote-Port	UDP port number of the session sender.

Display details about all measurement sessions.

```
<Huawei> display twamp-light responder test-session verbose
Session ID                  : 1
Local IP                    : 192.168.1.1
Local Port                  : 10000
Remote IP                   : 192.168.1.6
Remote Port                 : 20000
Mode                        : unauthenticated
VPN Instance                :
Description                 : test

Session ID                  : 2
Local IP                    : 192.168.1.2
Local Port                  : 10000
Remote IP                   : 192.168.1.6
Remote Port                 : 20000
Mode                        : unauthenticated
VPN Instance                :
Description                 : test
```

Table 21-80 Description of the **display twamp-light responder test-session verbose** command output

Item	Description
Session ID	Measurement session ID.
Local IP	IP address of the session reflector.
Local Port	UDP port number of the session reflector.
Remote IP	IP address of the session sender.
Remote Port	UDP port number of the session sender.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Mode	Authentication mode. The value **unauthenticated** indicates that authentication is disabled.
VPN Instance	L3VPN instance name.
Description	Measurement session description.

21.14.3 display twamp-light statistic-type

Function

The **display twamp-light statistic-type** command displays bidirectional delay or packet loss statistics of the TWAMP Light sessions.

Format

display twamp-light statistic-type { **twoway-delay** | **twoway-loss** } **test-session** *session-id*

Parameters

Parameter	Description	Value
twoway-delay	Displays statistics about bidirectional delay measurement.	–
twoway-loss	Displays statistics about bidirectional packet loss measurement.	–

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
test-session *session-id*	Displays statistics about the specified session.	The value is an integer. • For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. • For AR1200 series, the value ranges from 1 to 128. • For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. • For AR2240C, the value ranges from 1 to 256. • AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. • For AR3600 series, the value ranges from 1 to 1024.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view statistics on a measurement session, run this command. The command output contains bidirectional delay or packet loss statistics on the TWAMP Light session.

Example

Display bidirectional delay statistics on the specified measurement session.

```
<Huawei> display twamp-light statistic-type twoway-delay test-session 1
Latest two-way delay statistics(usec):
--------------------------------------------------------------------------------
    Index      Delay(Avg)    Jitter(Avg)       Tx-Jitter(Avg)    Rx-Jitter(Avg)
--------------------------------------------------------------------------------
    11027      0             0                 0                 0
    11028      0             0                 0                 0
    11029      4             4                 4                 4
    11030      1             1                 1                 1
    11031      1             1                 1                 1
    11032      1             1                 1                 1
    11033      0             0                 0                 0
    11034      1             1                 1                 1
    11035      2             2                 2                 2
```


Copyright © Huawei Technologies Co., Ltd.

```
  11036        2          2          2          2
  11037        0          0          0          0
  11038        2          2          2          2
  11039        1          1          1          1
  11040        0          0          0          0
  11041        0          0          0          0
  11042        0          0          0          0
  11043        0          0          0          0
  11044        1          1          1          1
  11045        3          3          3          3
  11046        0          0          0          0
  11047        1          1          1          1
  11048        0          0          0          0
  11049        0          0          0          0
  11050        0          0          0          0
  11051        1          1          1          1
  11052        0          0          0          0
  11053        5          5          5          5
  11054        7          7          7          7
  11055        0          0          0          0
  11056        1          1          1          1
------------------------------------------------------------------------------
Average Delay    :        1    Average Jitter   :        1
Maximum Delay    :        7    Maximum Jitter   :        7
Minimum Delay    :        0    Minimum Jitter   :        0
Average TxJitter :        1    Average RxJitter :        1
Maximum TxJitter :        7    Maximum RxJitter :        7
Minimum TxJitter :        0    Minimum RxJitter :        0
```

Table 21-81 Description of the **display twamp-light statistic-type twoway-delay** command output

Item	Description
Latest two-way delay statistics(usec)	Bidirectional delay measurement statistics, in microsecond.
Index	Statistics sequence number.
Delay(Avg)	Average delay.
Jitter(Avg)	Average jitter.
Tx-Jitter(Avg)	Average jitter on the sender.
Rx-Jitter(Avg)	Average jitter on the receiver.
Average Delay	Average delay.
Average Jitter	Average jitter.
Maximum Delay	Maximum delay.
Maximum Jitter	Maximum jitter.
Minimum Delay	Minimum delay.
Minimum Jitter	Minimum jitter.
Average TxJitter	Average jitter on the sender.
Average RxJitter	Average jitter on the receiver.
Maximum TxJitter	Maximum jitter on the sender.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Maximum RxJitter	Maximum jitter on the receiver.
Minimum TxJitter	Minimum jitter on the sender.
Minimum RxJitter	Minimum jitter on the receiver.

NOTE

- The statistics includes the packet sampling point and accumulative statistics. On-demand statistics includes the recent 100 sampling points and continual statistics includes the recent 30 sampling points.
- The delay, jitter, and unidirectional jitter are the average values of the sampling point.
- The maximum, minimum, and average values in on-demand and continual measurement are accumulative values, so it is a normal situation that the values exceed the acceptable range of the sampling point.
- The interval for displaying sampling result is relevant to the configured packet sending interval. If the sending interval is set to 100 ms, the sampling result is displayed every second. If the sending interval is set to 1000 ms, the sampling result is displayed every 10s.

Display bidirectional packet loss statistics on the specified measurement session.

```
<Huawei> display twamp-light statistic-type twoway-loss test-session 1
Latest two-way loss statistics:
--------------------------------------------------------------------------------
    Index      Loss count      Loss ratio
--------------------------------------------------------------------------------
    11006               5      50.0000%
    11007               3      30.0000%
    11008               4      40.0000%
    11009               8      80.0000%
    11010              10     100.0000%
    11011               1      10.0000%
    11012              10     100.0000%
    11013               2      20.0000%
    11014              10     100.0000%
    11015               9      90.0000%
    11016               6      60.0000%
    11017               2      20.0000%
    11018               8      80.0000%
    11019               2      20.0000%
    11020               8      80.0000%
    11021               2      20.0000%
    11022               2      20.0000%
    11023               7      70.0000%
    11024               4      40.0000%
    11025               4      40.0000%
    11026               7      70.0000%
    11027               7      70.0000%
    11028               8      80.0000%
    11029               1      10.0000%
    11030               2      20.0000%
    11031               8      80.0000%
    11032               7      70.0000%
    11033               7      70.0000%
    11034               8      80.0000%
    11035               4      40.0000%
--------------------------------------------------------------------------------
Average Loss Count :        5    Average Loss Ratio :  55.3333%
```

 Copyright © Huawei Technologies Co., Ltd.

```
Maximum Loss Count :       10    Maximum Loss Ratio : 100.0000%
Minimum Loss Count :        1    Minimum Loss Ratio :  10.0000%
```

Table 21-82 Description of the **display twamp-light statistic-type twoway-loss** command output

Item	Description
Latest two-way loss statistics	Bidirectional packet loss statistics.
Loss count	Number of dropped packets.
Loss ratio	Packet loss rate.
Average Loss Count	Average number of dropped packets.
Average Loss Ratio	Average packet loss rate.
Maximum Loss Count	Maximum number of dropped packets.
Maximum Loss Ratio	Maximum packet loss rate.
Minimum Loss Count	Minimum number of dropped packets.
Minimum Loss Ratio	Minimum packet loss rate.

NOTE

- The statistics includes the packet sampling point and accumulative statistics. On-demand statistics includes the recent 100 sampling points and continual statistics includes the recent 30 sampling points.
- The delay, jitter, and unidirectional jitter are the average values of the sampling point.
- The maximum, minimum, and average values in on-demand and continual measurement are accumulative values, so it is a normal situation that the values exceed the acceptable range of the sampling point.
- The interval for displaying sampling result is relevant to the configured packet sending interval. If the sending interval is set to 100 ms, the sampling result is displayed every second. If the sending interval is set to 1000 ms, the sampling result is displayed every 10s.

21.14.4 display twamp-light test-session

Function

The **display twamp-light test-session** command displays real-time information about TWAMP Light sessions.

Format

display twamp-light test-session [**verbose** | *session-id*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
verbose	Displays details about a TWAMP Light session.	-
session-id	Displays real-time information about the specified TWAMP Light session.	The value is an integer. • For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. • For AR1200 series, the value ranges from 1 to 128. • For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. • For AR2240C, the value ranges from 1 to 256. • AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. • For AR3600 series, the value ranges from 1 to 1024.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a fault occurs in continual measurement, on-demand measurement, or measurement session, run this command to view real-time information about the TWAMP Light sessions.

Example

Display the summary of all measurement sessions.

```
<Huawei> display twamp-light test-session
Total number  : 2
Active number : 1
------------------------------------------------------------------------------
  ID       Sender-IP   Sender-Port     Reflector-IP    Reflector-Port  State
------------------------------------------------------------------------------
  1        1.1.1.1         2001        2.2.2.2             2010    active
  2        1.1.1.1         2001        3.3.3.3             2020    inactive
```


Copyright © Huawei Technologies Co., Ltd.

Table 21-83 Description of the **display twamp-light test-session** command output

Item	Description
Total number	Total number of sessions.
Active number	Number of sessions in continual or on-demand measurement.
ID	Measurement session ID.
Sender-IP	IP address of the session sender.
Sender-Port	UDP port number of the session sender.
Reflector-IP	IP address of the session reflector.
Reflector-Port	UDP port number of the session reflector.
State	The states of measurement sessions include: ● active: indicates that continual or on-demand measurement is enabled. ● inactive: indicates that continual or on-demand measurement is not enabled or not normally enabled. – not startup: indicates that measurement is not enabled. – absence of resource: indicates that there is a lack of resources such as boards. – board fault: indicates a board failure. **NOTE** If the **State** value is active, the number of sent and received packets is the real-time result. If the **State** value is inactive, the number of sent and received packets is the last query result when the state is active.

Display details about all measurement sessions.

```
<Huawei> display twamp-light test-session verbose
Session ID                  : 1
State                       : active
Type                        : continual
Sender IP                   : 1.1.1.1
Sender Port                 : 2001
Reflector IP                : 2.2.2.2
Reflector Port              : 2010
Mode                        : unauthenticated
DSCP                        : 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Padding Length                : 128
VPN Instance                  :
Last Start Time               : 2014-08-05 16:41:05-08:00
Last Stop Time                : never
Period Time(in millisecond)   : 100
Time Out(in second)           : 5
Duration Time(in second)      : -
Packet Count                  : -
Sequence Number               : 0
Test Tx Number                : 0
Test Rx Number                : 0
Test Discard Number           : 0

Session ID                    : 2
State                         : inactive(absence of resource)
Type                          : on-demand
Sender IP                     : 1.1.1.1
Sender Port                   : 2001
Reflector IP                  : 3.3.3.3
Reflector Port                : 2020
Mode                          : unauthenticated
DSCP                          : 0
Padding Length                : 128
VPN Instance                  :
Last Start Time               : never
Last Stop Time                : never
Period Time(in millisecond)   : 100
Time Out(in second)           : 8
Duration Time(in second)      : 300
Packet Count                  : 0
Sequence Number               : 0
Test Tx Number                : 0
Test Rx Number                : 0
Test Discard Number           : 0
```

Table 21-84 Description of the **display twamp-light test-session verbose** command output

Item	Description
Session ID	Measurement session ID.
Type	Measurement session type: • on-demand • continual
Sender IP	IP address of the session sender.
Sender Port	UDP port number of the session sender.
Reflector IP	IP address of the session reflector.
Reflector Port	UDP port number of the session reflector.
Mode	Authentication mode. The value **unauthenticated** indicates that authentication is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DSCP	Differentiated Services Code Point (DSCP) value of the measurement session.
Padding Length	Padding length of the measurement session.
VPN Instance	L3VPN instance name.
Last Start Time	Latest activation time.
Last Stop Time	Latest stop time.
Period Time(in millisecond)	Measurement interval of a session, in millisecond.
Time Out(in second)	Timeout interval, in seconds.
Duration Time(in second)	Packet sending duration, displayed only for on-demand measurement, in seconds.
Packet Count	Number of sent packets, displayed only for on-demand measurement.
Sequence Number	Latest sequence number.
Test Tx Number	Accumulative number of sent packets.
Test Rx Number	Accumulative number of received packets.
Test Discard Number	Accumulative number of dropped invalid packets.

Display details about the specified measurement session.

```
<Huawei> display twamp-light test-session 1
Session ID                    : 1
State                         : active
Type                          : continual
Sender IP                     : 1.1.1.1
Sender Port                   : 2001
Reflector IP                  : 2.2.2.2
Reflector Port                : 2010
Mode                          : unauthenticated
DSCP                          : 0
Padding Length                : 128
VPN Instance                  :
Last Start Time               : 2014-08-05 16:41:05-08:00
Last Stop Time                : never
Period Time(in millisecond)   : 100
Time Out(in second)           : 5
Duration Time(in second)      : -
Packet Count                  : -
Sequence Number               : 0
Test Tx Number                : 0
Test Rx Number                : 0
Test Discard Number           : 0
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.14.8 test start

21.14.9 test start-continual

21.14.5 nqa twamp-light

Function

The **nqa twamp-light** command creates the TWAMP Light service and displays the TWAMP-Light view. If the TWAMP-Light service already exists, the TWAMP-Light view is directly displayed.

The **undo nqa twamp-light** command deletes the TWAMP Light service.

By default, the TWAMP Light service is not created.

Format

nqa twamp-light

undo nqa twamp-light

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

TWAMP Light uses a light structure to simplify the protocol used to set up performance measurement sessions. It measures bidirectional IP performance between any network nodes. When the TWAMP Light service is required, run the **nqa twamp-light** command to create the TWAMP Light service.

Precautions

After you run the **undo nqa twamp-light** command, the device automatically deletes all measurement sessions and services on client and sender.

Example

Create the TWAMP Light service.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light]
```


Copyright © Huawei Technologies Co., Ltd.

21.14.6 responder

Function

The **responder** command enables the TWAMP Light Responder function and displays the Responder view. If the Responder function has been enabled, this command directly displays the Responder view.

The **undo responder** command disables the TWAMP Light Responder function.

By default, the TWAMP Light Responder function is disabled.

Format

responder

undo responder

Parameters

None

Views

TWAMP-Light view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use the TWAMP Light service, run the **responder** command on the responder to display the responder view and create a measurement session. Then the controller starts the measurement service based on the session configuration.

Precautions

After the TWAMP Light responder is deleted, the packet loss rate is displayed as 100%, which is inaccurate.

Example

Enable the TWAMP Light responder function.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] responder
[Huawei-twamp-light-responder]
```


Copyright © Huawei Technologies Co., Ltd.

21.14.7 sender

Function

The **sender** command enables the TWAMP Light Sender function and displays the Sender view. If the Sender function has been enabled, this command directly displays the Sender view.

The **undo sender** command disables the TWAMP Light Sender function.

By default, the TWAMP Light Sender function is disabled.

Format

sender

undo sender

Parameters

None

Views

TWAMP-Light view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use the TWAMP Light service, create the TWAMP Light Sender using the **sender** command, and then start the measurement service on Sender.

Precautions

- When starting the measurement service, ensure that the TWAMP Light session has been created on the Client.
- When you delete the Sender, only the continual measurement service is stopped, but the on-demand measurement service will not be stopped. The on-demand measurement stops only when the specified interval is expired or a certain number of packets are sent.

Example

Display the Sender view.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] sender
[Huawei-twamp-light-sender]
```

 Copyright © Huawei Technologies Co., Ltd.

21.14.8 test start

Function

The **test start** command sets the time range or number of packets for the on-demand measurement service.

Format

test start test-session *session-id* { **duration** *duration* | **packet-count** *packet-count* } [**period** { **10** | **100** | **1000** | **30000** }] [**time-out** *time-out*]

Parameters

Parameter	Description	Value
test-session *session-id*	Specifies the ID of the measurement session.	The value is an integer. ● For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. ● For AR1200 series, the value ranges from 1 to 128. ● For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. ● For AR2240C, the value ranges from 1 to 256. ● AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. ● For AR3600 series, the value ranges from 1 to 1024.
duration *duration*	Specifies the packet sending duration of the measurement session.	The value is an integer that ranges from 60 to 300, in seconds.
packet-count *packet-count*	Specifies the number of packets sent in the measurement session.	The value is an integer that ranges from 100 to 30000.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
period	Specifies the interval for sending packets.	The value is an integer, in millisecond. The default value is 100 ms.
10	Sets the interval for sending packets to 10 ms.	-
100	Sets the interval for sending packets to 100 ms.	-
1000	Sets the interval for sending packets to 1s.	-
30000	Sets the interval for sending packets to 30s.	-
time-out *time-out*	Specifies the timeout interval for response packets within the sampling interval.	The value is an integer that ranges from 1 to 10, in seconds. By default, the value is 5s.

Views

TWAMP-Light-Sender view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

TWAMP Light includes two modes: on-demand and continual. On-demand measurement indicates that performance measurement is started manually within the specified time range aiming at network fault diagnosis. It is a one-off measurement in the diagnosis period. Continual measurement indicates the measurement is performed continuously.

- To measure performance only once, enable on-demand measurement by running the **test start** command. The measurement stops when the specified interval is expired or a certain number of packets are sent.
- To measure performance continuously, enable continual measurement by running the **test start-continual** command.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

A session has been created on Client.

Precautions

On-demand measurement fails in the following situations:

- More than 64 measurement sessions are configured.
- On-demand measurement is started during continual measurement.
- The measurement command is successfully executed, but the measurement fails to start due to a lack of resource, such as boards. In this situation, the **display twamp-light test-session** command displays the **State** value as inactive.

Example

Set the number of sent packets to 30000 to enable on-demand measurement.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] sender
[Huawei-twamp-light-sender] test start test-session 1 packet-count 30000
```

Related Topics

21.14.9 test start-continual

21.14.4 display twamp-light test-session

21.14.9 test start-continual

Function

The **test start-continual** command configures continual measurement.

The **undo test start-continual** command stops continual measurement.

Format

test start-continual test-session *session-id* [**period** { **10** | **100** | **1000** | **30000** } [**sample-interval** *interval-value*]] [**time-out** *time-out*]

undo test start-continual test-session *session-id*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
test-session *session-id*	Specifies the ID of the measurement session.	The value is an integer. • For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. • For AR1200 series, the value ranges from 1 to 128. • For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. • For AR2240C, the value ranges from 1 to 256. • AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. • For AR3600 series, the value ranges from 1 to 1024.
period	Specifies the interval for sending packets.	The value is an integer, in millisecond. The default value is 100 ms.
10	Sets the interval for sending packets to 10 ms.	-
100	Sets the interval for sending packets to 100 ms.	-
1000	Sets the interval for sending packets to 1s.	-
30000	Sets the interval for sending packets to 30s.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
sample-interval *interval-value*	Specifies a sampling interval.	The value is an integer, in seconds. **NOTE** The sampling interval varies according to the interval at which packets are sent over a test session. • If the packet sending interval is 10 ms, the sampling interval is 1s. • If the packet sending interval is 100 ms, the sampling interval ranges from 1s to 10s, with the default value being 1s. • If the packet sending interval is 1s, the sampling interval ranges from 10s to 100s, with the default value being 10s. • If the packet sending interval is 30s, the sampling interval ranges from 60s to 300s, with the default value being 60s. **sample-interval** *interval-value* must be less than or equal to **duration** *duration*.
time-out *time-out*	Specifies the timeout interval for response packets within the sampling interval.	The value is an integer that ranges from 1 to 10, in seconds. By default, the value is 5s.

Views

TWAMP-Light-Sender view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

TWAMP Light includes two modes: on-demand and continual. On-demand measurement indicates that performance measurement is started manually within the specified time range aiming at network fault diagnosis. It is a one-off measurement in the diagnosis period. Continual measurement indicates the measurement is performed continuously.

- To measure performance only once, enable on-demand measurement by running the **test start** command. The measurement stops when the specified interval is expired or a certain number of packets are sent.
- To measure performance continuously, enable continual measurement by running the **test start-continual** command.

Prerequisites

A session has been created on Client.

Copyright © Huawei Technologies Co., Ltd.

Precautions

- When a measurement session is deleted, the continual measurement configuration of this session is also deleted.
- After the Sender is deleted, all continual measurement configurations are deleted.
- If you enable continual measurement during an on-demand measurement, the on-demand measurement immediately stops and the continual measurement starts.
- The measurement command is successfully executed, but the measurement fails to start due to a lack of resource, such as boards. In this situation, the **display twamp-light test-session** command displays the **State** value as inactive.

Example

Start continual measurement for a session.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] sender
[Huawei-twamp-light-sender] test start-continual test-session 1
```

Related Topics

21.14.8 test start

21.14.4 display twamp-light test-session

21.14.10 test stop

Function

The **test stop** command stops on-demand measurement of the TWAMP Light service.

Format

test stop { **all** | **test-session** *session-id* }

Parameters

Parameter	Description	Value
all	Stops on-demand measurement for all sessions.	–

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
test-session *session-id*	Specifies the ID of the measurement session to be stopped.	The value is an integer. • For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. • For AR1200 series, the value ranges from 1 to 128. • For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. • For AR2240C, the value ranges from 1 to 256. • AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. • For AR3600 series, the value ranges from 1 to 1024.

Views

TWAMP-Light-Sender view

Default Level

2: Configuration level

Usage Guidelines

To stop on-demand measurement for the specified session or all sessions, you can run the **test stop** command.

Example

Stop on-demand measurement for session 1.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] sender
[Huawei-twamp-light-sender] test stop test-session 1
```

21.14.11 test-session

Function

The **test-session** command creates a session in the TWAMP Light service.

The **undo test-session** command deletes a session in the TWAMP Light service.

By default, no measurement session is created.

Copyright © Huawei Technologies Co., Ltd.

Format

test-session *session-id* **sender-ip** *sender-ip-address* **reflector-ip** *reflector-ip-address* **sender-port** *sender-port* **reflector-port** *reflector-port* [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **padding** *padding-length* | **description** *description*] *

undo test-session *session-id*

Parameters

Parameter	Description	Value
session-id	Specifies the ID of the measurement session.	The value is an integer. • For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. • For AR1200 series, the value ranges from 1 to 128. • For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. • For AR2240C, the value ranges from 1 to 256. • AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. • For AR3600 series, the value ranges from 1 to 1024.
sender-ip *sender-ip-address*	Specifies the IP address of the sender.	The value is in dotted decimal notation.
reflector-ip *reflector-ip-address*	Specifies the IP address of the reflector.	The value is in dotted decimal notation.
sender-port *sender-port*	Specifies the UDP port number of the sender.	The value is 862, 863, or an integer that ranges from 1025 to 65535.
reflector-port *reflector-port*	Specifies the UDP port number of the reflector.	The value is 862, 863, or an integer that ranges from 1025 to 65535.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
dscp *dscp-value*	Specifies the DSCP value of sent packets.	The value is an integer that ranges from 0 to 63. The default value is 0.
padding *padding-length*	Specifies the padding length of the measurement session.	The value is an integer that ranges from 32 to 8500. The default value is 128.
description *description*	Indicates the description of the specified measurement session. To configure description for a measurement session, specify the **description** parameter. The description facilitates session management and operation.	The value is a string of 3 to 32 characters without spaces. **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

TWAMP-Light-Client view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you need to use the TWAMP Light service, create a TWAMP Light session, including the sender's IP address, reflector's IP address, sender's UDP port number, reflector's UDP port number, and VPN instance name. The created session starts measurement only when the start command is run.

Precautions

- After a session is created, its parameters cannot be modified. To modify the session parameters, delete the session and create it again.

Copyright © Huawei Technologies Co., Ltd.

- The IP address must be a unicast address.
- The UDP port of the sender must be a port that is not occupied.
- All the parameters related to the VPN instance must exist. When the VPN instance is deleted, the related measurement instance is also deleted.
- To configure a session with multiple DSCP values, you can specify different UDP port numbers for sender. The following are two examples:
  - Session 1: **test-session** 1 **sender-ip** 1.1.1.1 **reflector-ip** 2.2.2.2 **sender-port** 1025 **reflector-port** 1025 **dscp** 3
  - Session 2: **test-session** 2 **sender-ip** 1.1.1.1 **reflector-ip** 2.2.2.2 **sender-port** 1026 **reflector-port** 1025 **dscp** 6

Example

Create a TWAMP Light session.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] client
[Huawei-twamp-light-client] test-session 1 sender-ip 1.1.1.1 reflector-ip 2.2.2.2 sender-port 3000 reflector-port 3000
```

21.14.12 test-session (TWAMP-Light-Responder view)

Function

The **test-session** command creates a session on the TWAMP Light reflector.

The **undo test-session** command deletes a session on the TWAMP Light reflector.

By default, no measurement session is created on the reflector.

Format

test-session *session-id* **local-ip** *local-ip-address* **remote-ip** *remote-ip-address* **local-port** *local-port* **remote-port** *remote-port* [**vpn-instance** *vpn-instance-name*] [**description** *description*]

undo test-session *session-id* [**local-ip** *local-ip-address* **remote-ip** *remote-ip-address* **local-port** *local-port* **remote-port** *remote-port* [**vpn-instance** *vpn-instance-name*] [**description** *description*]]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
session-id	Specifies the ID of the measurement session.	The value is an integer. • For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. • For AR1200 series, the value ranges from 1 to 128. • For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. • For AR2240C, the value ranges from 1 to 256. • AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. • For AR3600 series, the value ranges from 1 to 1024.
local-ip *local-ip-address*	Specifies the IP address of the reflector.	The value is in dotted decimal notation.
remote-ip *remote-ip-address*	Specifies the IP address of the sender.	The value is in dotted decimal notation.
local-port *local-port*	Specifies the UDP port number of the reflector.	The value is 862, 863, or an integer that ranges from 1025 to 65535.
remote-port *remote-port*	Specifies the UDP port number of the sender.	The value is 862, 863, or an integer that ranges from 1025 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
description *description*	Indicates the description of the specified measurement session. To configure description for a measurement session, specify the **description** parameter. The description facilitates session management and operation.	The value is a string of 3 to 32 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

TWAMP-Light-Responder view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you need to use the TWAMP Light service, create a TWAMP Light session on the reflector, including the sender's IP address, reflector's IP address, sender's UDP port number, reflector's UDP port number, and VPN instance name.

Precautions

- The created session starts measurement only when the start command is run.
- After a measurement session is created, its parameters cannot be modified.
- The IP address must be a unicast address.
- The UDP port of the sender must be a port that is not occupied.
- The VPN instance parameters must already exist.

Example

Create a TWAMP Light session on the reflector.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] responder
[Huawei-twamp-light-responder] test-session 1 local-ip 1.1.1.1 remote-ip 2.2.2.2 local-port 3000 remote-port 3000 vpn-instance vpn1
```

 Copyright © Huawei Technologies Co., Ltd.

21.15 Ping and Tracert Configuration Commands

21.15.1 ping

Function

The **ping** command checks whether a specified IPv4 address is reachable and exports corresponding statistics.

Format

ping [**ip**] [**-a** *source-ip-address* | **-c** *count* | **-d** | **-h** *ttl-value* | { **-nexthop** *nexthop-ip-address* | **-i** *interface-type interface-number* } * | **-m** *time* | **-n** | **-name** | **-p** *pattern* | **-q** | **-r** | { **-s** *packetsize* | **-range** [**min** *min-size* | **max** *max-size* | **step** *step-size*] * } | **-system-time** | **-t** *timeout* | **-tos** *tos-value* | **-v** | **-vpn-instance** *vpn-instance-name* | [**-f** | **ignore-mtu**]] * *host* [**ip-forwarding**]

Parameters

Parameter	Description	Value
ip	Indicates the IPv4 protocol. If **ip** is not specified, the IPv4 protocol is used.	-
-a *source-ip-address*	Specifies the source IP address of the ICMP Echo Request message. If the source IP address is not specified, the IP address of the outbound interface is used as the source IP address of the ICMP Echo Request message.	The value is in dotted decimal notation. The IP address must be a valid A, B, or C class address.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-c *count*	Specifies the number of times for sending ICMP Echo Request messages. The **ping** command labels each ICMP Echo Request message with a sequence ID that starts from 1 and is increased by 1. By default, five ICMP Echo Request messages are sent. You can set the number of ICMP Echo Request messages to send by specifying the parameter *count*. In the case of poor network quality, you can set this parameter to a comparatively large value to check the network quality based on the packet loss rate.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-d	Indicates that the socket works in debug mode.	By default, the socket works in non-debug mode.
-f	Indicates that packets are not fragmented during transmission. **NOTE** After this parameter is specified, ICMP packets are not fragmented. If the ICMP packet size exceeds the link MTU, the ICMP packet is discarded. If you do not want ICMP packets to be discarded, do not specify this parameter or increase the link MTU.	-
-h *ttl-value*	Specifies the TTL value. If the TTL field is reduced to 0 during message forwarding, the Layer 3 device that the message reaches sends an ICMP timeout message to the source host, indicating that the destination host is unreachable.	The value is an integer that ranges from 1 to 255. The default value is 255.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-nexthop *nexthop-ip-address*	Specifies an IP address for the next hop. If you have specified this parameter, the device no longer searches the routing table before sending ICMP Echo Request packets. This process prevents ping failures caused by incorrect routing entries.	The value is in dotted decimal notation. **NOTE** • The specified next hop address must be the next hop address of a directly connected physical interface. • When you specify a next hop address, you can configure **-i** *interface-type interface-number* to specify an outbound interface. The following conditions must be met to ensure a test success: • The specified next hop address must match the outbound interface. • The specified outbound interface cannot be a logical interface's member interface. • If you have specified a next hop address, you cannot specify a VPN.
-i *interface-type interface-number*	Specifies the outbound interface for sending ICMP Echo Request messages.	**NOTE** • In load balancing scenarios, if an interface is specified to send ICMP Echo Request packets, all packets are sent from the interface and load balancing is not performed. • The interface specified to send ICMP Echo Request packets must be a Layer 3 interface, such as a VLANIF interface, Eth-trunk interface, or a Layer 3 Eth-trunk member interface.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-m *time*	Specifies the time to wait before sending the next ICMP Echo Request message. Each time the source sends an ICMP Echo Request message using the **ping** command, the source waits a period of time (500 ms by default) before sending the next ICMP Echo Request message. You can set the time to wait before sending the next ICMP Echo Request message using the parameter *time*. In the case of poor network condition, the value should be equal to or larger than 500, in milliseconds.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 500.
-n	Uses the value of *host* as the IP address to spare domain name resolution.	-
-name	Displays the name of the destination host.	-
-p *pattern*	Specifies pad characters for ICMP Echo Request messages. By configuring pad characters for ICMP Echo Request messages, you can identify a specific message among the large number of received ICMP Echo Reply messages.	The value is a hexadecimal integer that ranges from 0 to FFFFFFFF. By default, the padding starts from 0x01, and continues in ascending order.
-q	Displays only the statistics. If the **ping** command carries this parameter, the system displays only the statistics information such as the number of sent and received packets, packet loss rate, and minimum, average, and maximum RTTs of the packet.	By default, the system displays all statistics information.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-r	Records the route along which an IP packet is forwarded. When **-r** is specified, during the transmission of an IP packet, the IP address of each Layer 3 device that the IP packet passes through is added to the Options field. When the IP packet reaches the destination, all IP addresses recorded in the Options field are copied to the ICMP Echo Reply message. In addition, the IP address of each Layer 3 device that the returned IP packet passes through is added to the message. When the ping program receives the ICMP Echo Reply message, IP addresses of the passed Layer 3 devices are displayed.	By default, the route along which an IP packet is forwarded is not recorded.
-s *packetsize*	Specifies the length of an ICMP Echo Request message, excluding the IP header and ICMP header.	The value is an integer that ranges from 20 to 9600, in bytes. The default value is 56.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-range	Enables the device to send ICMP Echo Request messages with variable payload lengths.	• If the **-range** parameter is not specified, the payload length of an ICMP Echo Request message is equal to the length specified by the **-s** *packetsize* parameter. The default value is 56, in bytes. • If the **-range** parameter is specified, the payload length of the first ICMP Echo Request message is **min** *min-size*, and that of the second ICMP Echo Request message is **min** *min-size* plus **step** *step-size*. The payload length increases incrementally by **step** *step-size* for subsequent ICMP Echo Request messages until **max** *max-size* is reached. After that, the device will not send ICMP Echo Request messages any more. By default, the payload length of an ICMP Echo Request message ranges from 56 to 9600 bytes, and the step length is 1 byte.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		NOTE • The command execution takes a long period if a large number of ICMP Echo Request messages need to be sent. If you want to terminate the command execution, press **Ctrl+C**. • To change the number of ICMP Echo Request messages to be sent, change the values of **min** *min-size* and **max** *max-size*. The value of **min** *min-size* must be smaller than that of **max** *max-size*. • If both the **-range** and **-c** *count* parameters are specified, the device sends ICMP Echo Request messages of the same payload length for the number of times specified by the **-c** *count* parameter.
min *min-size*	Specifies the minimum payload length of an ICMP Echo Request message.	The value is an integer ranging from 20 to 9600, in bytes. The default value is 56.
max *max-size*	Specifies the maximum payload length of an ICMP Echo Request message.	The value is an integer ranging from 20 to 9600, in bytes. The default value is 9600.
step *step-size*	Specifies the step length of an ICMP Echo Request message.	The value is an integer ranging from 1 to 1000, in bytes. The default value is 1.
-system-time	Displays the system time when the ping packet is sent.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-t *timeout*	Specifies the timeout period to wait for an ICMP Echo Reply message after an ICMP Echo Request message is sent. After the **ping** command is run, the source sends an ICMP Echo Request message to a destination and waits for an ICMP Echo Reply message. If the destination, after receiving the ICMP Echo Request message, returns an ICMP Echo Reply message to the source within the period specified by the parameter *timeout*, the destination is reachable. If the destination does not return an ICMP Echo Reply message within the specified period, the source displays information indicating that the message times out. Normally, the source receives an ICMP Echo Reply message within 1 to 10 seconds after sending an ICMP Echo Request message. If the transmission speed is low, properly prolong the timeout period.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.
-tos *tos-value*	Specifies the ToS value of the sent ICMP Echo Request messages. The ToS value is used to set the packet priority.	The value is an integer that ranges from 0 to 255. The default value is 0.
-v	Displays all received ICMP Echo Reply messages. • If **-v** is not specified, the system displays only the ICMP Echo Reply messages received by the local user. • If **-v** is specified, the system displays all received ICMP Echo Reply messages.	By default, only ICMP Echo Reply messages for the local user are displayed.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ignore-mtu	Indicates that the system does not check the interface MTU when a packet is sent.	-
host	Specifies the domain name or IP address of the destination host.	The value is a string of 1 to 255 case-sensitive characters with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Alternatively, the value can be a valid IPv4 address in dotted decimal notation.
ip-forwarding	Indicates that the ping packets are forcibly forwarded through IP on the first node.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

The **ping** command is a common debugging tool for testing the network connectivity by transmitting ICMP Echo messages. It can detect the following items:

- Availability of the remote device
- Round-trip delay in communication between the local and remote devices
- Packet loss rate

You can run the **ping** command to check the network connectivity or line quality in the following scenarios:

- Check the protocol stack on the local device. You can run the **ping** *loopback-address* command to check whether the TCP/IP protocol stack works properly on the local device.

 Copyright © Huawei Technologies Co., Ltd.

- Check whether the destination host is reachable on an IP network. You can run the **ping** *host* command to send an ICMP Echo Request message to the destination host. If a reply is received, the destination host is reachable.
- Check whether the peer is reachable on a Layer 3 VPN. On a Layer 3 VPN, devices may not have routing information about each other. Therefore, you cannot use the **ping** *host* command to check whether the peer is reachable. When a VPN instance name is specified, you can run the **ping -vpn-instance** *vpn-instance-name host* command to send an ICMP Echo Request message to the peer. If the peer returns an ICMP Echo Reply message, the peer is reachable.
- In the case of an unstable network, you can run the **ping -c** *count* **-t** *timeout host* command to check the quality of the network between the local device and the peer. By analyzing the packet loss rate and average delay in the command output, you can evaluate the network quality. If the network is unreliable, set the packet transmission count (**-c**) and timeout (**-t**) to the upper limits. This makes the test result accurate.
- Check the path. You can run the **ping -r** *host* command to obtain information about nodes along the path from the local device to the peer.
- When you want to locate a fault or collect traffic statistics, specify the **-m** and **-t** parameters to allow the device to quickly send **ping** request packets.
- When the packet size is large, specify the **-s** and **-f** parameters to detect the MTU on the intermediate link.
- When IPSec or NAT is used, specify the **-a** parameter to configure the source address as the private network address to check the network connectivity. In addition, to check whether NAT translation succeeds using the ping test with the source address specified, you must run the **ip soft-forward enhance enable** command first to enable the enhanced forwarding function for control packets generated by the device.

Prerequisite

- Before running the **ping** command, ensure that the ICMP module is working properly.
- If **-vpn-instance** is specified, ensure that the VPN module is working properly.

Precautions

- When you use the **ping** command on a third-party device to check the connectivity between the third-party device and the router, set the ping packet size to a value smaller than 64000 bytes to ensure a better test result.
- If an intermediate device is disabled from responding to ICMP messages, detection on this node fails.
- If a fault occurs in the ping process, you can press **Ctrl+C** to terminate the ping operation.
- For security purposes, do not **ping** the broadcast address, such as XX.XX.XX.255.
- When the destination host is unreachable, the system displays "Request time out", which indicates that the ICMP Echo Request message times out.

Example

Check whether the host at 10.1.1.2 is reachable.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> ping 10.1.1.2
  PING 10.1.1.2: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.1.1.2: bytes=56 Sequence=5 ttl=255 time=1 ms
  --- 10.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

Check whether the device at 10.1.1.3 in vpn1 is reachable

```
<Huawei> ping -vpn-instance vpn1 10.1.1.3
  PING 10.1.1.3: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.3: bytes=56 Sequence=1 ttl=255 time=31 ms
    Reply from 10.1.1.3: bytes=56 Sequence=2 ttl=255 time=31 ms
    Reply from 10.1.1.3: bytes=56 Sequence=3 ttl=255 time=31 ms
    Reply from 10.1.1.3: bytes=56 Sequence=4 ttl=255 time=31 ms
    Reply from 10.1.1.3: bytes=56 Sequence=5 ttl=255 time=31 ms
  --- 10.1.1.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 31/31/31 ms
```

Check whether the host at 10.1.1.4 is reachable, set the transmission count to 8, and set the period for waiting for an ICMP Echo Reply message to 4000 ms.

```
<Huawei> ping -c 8 -t 4000 10.1.1.4
  PING 10.1.1.4: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.4: bytes=56 Sequence=1 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=2 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=3 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=4 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=5 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=6 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=7 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=8 ttl=255 time=32 ms
  --- 10.1.1.4 ping statistics ---
    8 packet(s) transmitted
    8 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 32/32/32 ms
```

Table 21-85 Description of the ping command output

Item	Description
PING x.x.x.x	Reachability of the destination host with the IP address as *x.x.x.x* is tested.
x data bytes	Length of a sent ICMP Echo Request message.
press CTRL_C to break	The ongoing ping test is terminated after you press **Ctrl +C**.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reply from x.x.x.x	The destination host responds to the ICMP Echo Request message with an ICMP Echo Reply message that contains the following items: • bytes: indicates the length of the ICMP Echo Reply message. • Sequence: indicates the sequence number of the ICMP Echo Reply message. • ttl: indicate the TTL value of the ICMP Echo Reply message. • time: indicates the RTT, in milliseconds. If no ICMP Echo Reply message is received after the timeout period, the system displays "Request time out".
x.x.x.x ping statistics	Statistics collected after the ping test on the destination host. The statistics include the following information: • packet(s) transmitted: indicates the number of sent ICMP Echo Request messages. • packet(s) received: indicates the number of received ICMP Echo Reply messages. • % packet loss: indicates the percentage of unresponded messages to total sent messages. • round-trip min/avg/max: indicates the minimum, average, and maximum RTTs. The unit is ms. (On an IPv4 network, round-trip min/avg/max is not displayed if the ping fails. On an IPv6 network, round-trip min/avg/max = 0/0/0 ms is displayed if the ping fails.)

Related Topics

21.15.2 ping ipv6
21.15.3 tracert
21.15.4 tracert ipv6

21.15.2 ping ipv6

Function

The **ping ipv6** command checks whether a specified IPv6 address is reachable and exports corresponding statistics.

Format

ping ipv6 [**-a** *source-ipv6-address* | **-c** *count* | **-h** *ttl-value* | **-m** *time* | **-name** | **-s** *packetsize* | **-t** *timeout* | **-tc** *traffic-class-value* | **vpn-instance** *vpn-instance-name*] * *host* [**-i** *interface-type interface-number*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
-a *source-ipv6-address*	Specifies a source IPv6 address for sending ICMPv6 Echo Request messages. The specified source IPv6 address cannot be the virtual IPv6 address configured for VRRP6. If no source IPv6 address is specified, the IPv6 address of the outbound interface is used as the source address for sending ICMPv6 Echo Request messages.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
-c *count*	Specifies the number of times for sending ICMPv6 Echo Request messages. You can increase the number of outgoing packets to detect the network quality based on the packet loss rate.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-h *ttl-value*	Specifies the TTL value. If the TTL field is reduced to 0 during message forwarding, the Layer 3 router that the message reaches sends an ICMPv6 timeout message to the source host, indicating that the destination host is unreachable.	The value is an integer that ranges from 1 to 255. The default value is 255.
-m *time*	Specifies the time to wait before sending the next ICMPv6 Echo Request message. Each time the source sends an ICMPv6 Echo Request message using the **ping ipv6** command, the source waits a period of time (2000 ms by default) before sending the next ICMPv6 Echo Request message. You can set the time to wait before sending the next ICMPv6 Echo Request message using the parameter *time*. In the case of poor network condition, the value should be equal to or larger than 2000, in milliseconds.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-name	Displays the name of the destination host.	-
-s *packetsize*	Specifies the length of an ICMPv6 Echo Request message, excluding the IP header and ICMPv6 header.	The value is an integer that ranges from 20 to 9600, in bytes. The default value is 56.
-t *timeout*	Specifies the timeout period to wait for an ICMPv6 Echo Reply message after an ICMPv6 Echo Request message is sent. After the **ping ipv6** command is run, the source sends an ICMPv6 Echo Request message to a destination and waits for an ICMPv6 Echo Reply message. If the destination, after receiving the ICMPv6 Echo Request message, returns an ICMPv6 Echo Reply message to the source within the period specified by the parameter *timeout*, the destination is reachable. If the destination does not return an ICMPv6 Echo Reply message within the specified period, the source displays information indicating that the message times out. Normally, the source receives an ICMPv6 Echo Reply message within 1 to 10 seconds after sending an ICMPv6 Echo Request message. If the transmission speed is low, properly prolong the timeout period.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.
-tc *traffic-class-value*	Specifies the traffic classification in the ICMPv6 Echo Request message. To configure traffic control for ICMPv6 packets, set the parameter *traffic-class-value*.	The value is an integer that ranges from 0 to 255. The default value is 0.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance for the IPv6 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
host	Specifies the host name or IPv6 address of the destination host.	The value is a string of 1 to 255 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. The IPv6 address is a 32–bit string in hexadecimal format, namely, the format X:X:X:X:X:X:X:X.
-i *interface-type interface-number*	Specifies the outbound interface for sending ICMPv6 Echo Request messages.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

The **ping ipv6** command is a widely used debugging tool for checking network connectivity and host reachability on an IPv6 network by transmitting ICMPv6 messages. It can detect the following items:

- Availability of the remote device
- Round-trip delay in communication between the local and remote devices
- Packet loss rate

You can run the **ping ipv6** command to check the IPv6 network connectivity or line quality in the following scenarios:

- Check the protocol stack on the local device. You can run the **ping ipv6** *IPv6-loopback-address* command to check whether the TCP/IP protocol stack works properly on the local device.
- Check whether the destination IPv6 host is reachable on an IPv6 network. You can run the **ping ipv6** *host* command to send an ICMPv6 Echo Request message to the destination host. If a reply is received, the destination host is reachable.
- Check whether the peer is reachable on a Layer 3 VPN. On a Layer 3 VPN, devices may not have routing information about each other. Therefore, you cannot use the **ping ipv6** *host* command to check whether the peer is reachable. When a VPN instance name is specified, you can run the **ping ipv6 vpn-instance** *vpn-instance-name host* command to send an ICMPv6 Echo

 Copyright © Huawei Technologies Co., Ltd.

Request message to the peer. If the peer returns an ICMPv6 Echo Reply message, the peer is reachable.

- In the case of an unstable network, you can run the **ping ipv6 -c** *count* **-t** *timeout host* command to check the quality of the network between the local device and the peer. By analyzing the packet loss rate and average delay in the command output, you can evaluate the network quality. If the network is unreliable, set the packet transmission count (**-c**) and timeout (**-t**) to the upper limits. This makes the test result accurate.

Prerequisites

- Before running the **ping ipv6** command, ensure that the ICMPv6 module is working properly.
- If **-vpn-instance** is specified, ensure that the VPN module is working properly.

Precautions

- If an intermediate device is disabled from responding to ICMPv6 messages, detection on this node fails.
- If the IPv6 address of the destination host maps the local address, specify the name of the local outbound interface through which the ICMPv6 Echo Request message is sent. Otherwise, reply to the **ping ipv6** command times out.
- When the destination host is unreachable, the system displays "Request time out" indicating that the ICMPv6 Echo Request message times out and displays statistics collected by the IPv6 ping test.
- If a fault occurs in the IPv6 ping process, you can press **Ctrl+C** to terminate the IPv6 ping operation.

Example

Check whether the host with the IPv6 address as FC00::1 is reachable.

```
<Huawei> ping ipv6 FC00::1
 PING FC00::1 : 56  data bytes, press CTRL_C to break
    Reply from FC00::1
    bytes=56 Sequence=1 hop limit=64 time=115 ms
    Reply from FC00::1
    bytes=56 Sequence=2 hop limit=64 time=1 ms
    Reply from FC00::1
    bytes=56 Sequence=3 hop limit=64 time=1 ms
    Reply from FC00::1
    bytes=56 Sequence=4 hop limit=64 time=1 ms
    Reply from FC00::1
    bytes=56 Sequence=5 hop limit=64 time=1 ms
  ---FC00::1 ping statistics---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max=1/23/115 ms
```

Table 21-86 Description of the ping ipv6 command output

Item	Description
PING HH:HH::HH:H	IPv6 address of the destination host.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
x data bytes	Length of a sent ICMPv6 Echo Request message.
press CTRL_C to break	The ongoing IPv6 ping test is terminated after you press **Ctrl+C**.
Reply from HH:HH::HH:H	The destination host responds to the ICMPv6 Echo Request message with an ICMPv6 Echo Reply message that contains the following items: • bytes: indicates the length of the ICMPv6 Echo Reply message. • sequence: indicates the sequence number of the ICMPv6 Echo Reply message. • hop limit: indicates the TTL of the ICMPv6 Echo Reply message. • time: indicates the RTT, in milliseconds. If no ICMPv6 Echo Reply message is received after the timeout period, the system displays "Request time out".
HH:HH::HH:H ping statistics	Statistics collected after the IPv6 ping test on the destination host. The statistics include the following information: • packet(s) transmitted: indicates the number of sent ICMPv6 Echo Request messages. • packet(s) received: indicates the number of received ICMPv6 Echo Reply messages. • % packet loss: indicates the percentage of unresponded messages to total sent messages. • round-trip min/avg/max: indicates the minimum, average, and maximum RTTs.

Related Topics

21.15.4 tracert ipv6

21.15.3 tracert

Function

The **tracert** command checks the path of packets from the source to the destination, checks network connectivity, and locates a network fault.

Format

tracert [**-a** *source-ip-address* | **-f** *first-ttl* | **-m** *max-ttl* | **-name** | **-p** *port* | **-q** *nqueries* | **-s** *packetsize* | **-v** | **-vpn-instance** *vpn-instance-name* [**pipe**] | **-w** *timeout*] * *host*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source address of a probe packet. If this parameter is not specified, the IP address of the outbound interface is used as the source IP address for sending tracert packets.	The value is in dotted decimal notation.
-f *first-ttl*	Specifies the initial TTL. The TTL field is carried in the IP header. It indicates the lifetime of packets and specifies the maximum hops that packets can pass through. The TTL value is set on the source and reduced by 1 each time the packet passes through a hop. When the TTL value is reduced to 0, the packet is discarded. At the same time, an ICMP Timeout message is sent to notify the source host. If *first-ttl* is specified and the number of hops is smaller than the value of *first-ttl*, no ICMP Timeout packet is sent to the source host when the packet passes through these hops. If *max-ttl* is specified, the value of *first-ttl* must be smaller than the value of *max-ttl*.	The value is an integer that ranges from 1 to 255. The default value is 1.
-m *max-ttl*	Specifies the maximum TTL. Usually, the maximum TTL is set to the number of hops the packet passes through. You need to use this parameter to change the TTL. If *first-ttl* is specified, the value of *max-ttl* must be greater than the value of *first-ttl*.	The value is an integer that ranges from 1 to 255. The default value is 30.
-name	Displays the host name of each hop.	-
-p *port*	Specifies the UDP port number of the destination. Before specifying the UDP port number for the destination, ensure that the port is not in use; otherwise, the tracert fails.	The value is an integer that ranges from 0 to 65535. The default value is 33434.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-q *nqueries*	Specifies the number of probe packets to be sent each time. In the case of poor network quality, you can set this parameter to a comparatively large value to ensure that the probe packet can reach the destination.	The value is an integer that ranges from 1 to 65535. The default value is 3.
-v	Displays the MPLS label carried in the ICMP Time Exceeded packet. This parameter is used to show the public label in the tracert initiated by PE.	By default, the MPLS label carried in the ICMP Time Exceeded is not displayed. Instead, only the path information carried in the ICMP Time Exceeded and Port-Unreachable packets is displayed.
-vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the destination address belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
pipe	Indicates that the TTL of a VPN instance is in pipe mode.	-
-w *timeout*	Specifies the timeout period to wait for a reply. If a tracert packet times out when reaching a gateway, an asterisk (*) is displayed. In the case of poor network quality and a low network transmission rate, you are advised to prolong the timeout period.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 5000.
-s *packetsize*	Specifies the length of an ICMP Echo Request message, excluding the IP header and ICMP header.	The value is an integer that ranges from 12 to 9600, in bytes. The default value is 12.
host	Indicates the domain name or IPv4 address of the destination host.	The value is a string of 1 to 255 case-sensitive characters with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Alternatively, the value can be a valid IPv4 address in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

During routine system maintenance, you can run the **ping** command to check network connectivity. If the ping fails, run the **tracert** command to locate the fault on the network.

You can specify different parameters in the **tracert** command for different scenarios:

- To check information about nodes between the source and the destination, run the **tracert** *host* command.
- To check information about nodes between the source and the destination on a Layer 3 VPN, run the **tracert -vpn-instance** *vpn-instance-name host* command. On a Layer 3 VPN, devices may not have routing information about each other. Therefore, you cannot use the **tracert** *host* command to check whether the peer is reachable. To check information about nodes between the source and the destination in a specified VPN instance, run the **tracert -vpn-instance** *vpn-instance-name host* command.
- On an unstable network, you can run the **tracert -q** *nqueries* **-w** *timeout host* command to check information about nodes between the source and the destination. If the network is unreliable, set the packet transmission count (**-q**) and timeout (**-w**) to the upper limits. This makes the test result accurate.
- To check information about nodes along a segment of a path, run the **tracert -f** *first-ttl* **-m** *max-ttl host* command that has initial TTL and maximum TTL specified.

Prerequisite

- The UDP module of each node is working properly; otherwise, the tracert operation fails.
- If **-vpn-instance** is specified, ensure that the VPN module of each node is working properly.
- The ICMP module of each node is working properly; otherwise, " * * * " is displayed.

Procedure

The execution process of the **tracert** command is as follows:

1. The source sends a packet with the TTL being 1. After the TTL times out, the first hop sends an ICMP Error message to the source, indicating that the packet cannot be forwarded.
2. The source sends a packet with the TTL being 2. After the TTL times out, the second hop sends an ICMP Error message to the source, indicating that the packet cannot be forwarded.

Copyright © Huawei Technologies Co., Ltd.

3. The source sends a packet with the TTL being 3. After the TTL times out, the third hop sends an ICMP Error message to the source, indicating that the packet cannot be forwarded.
4. The preceding process proceeds until the packet reaches the destination.

When receiving a packet, each destination hop cannot find the port specified in the packet, and returns an ICMP Port Unreachable message, indicating that the destination port is unreachable and the tracert ends. In this manner, the result of each probe is displayed on the source, according to which you can find the path from the source to the destination.

Configuration Impact

If a fault occurs when you run the **tracert** command, the following information may be displayed:

- !H: The host is unreachable.
- !N: The network is unreachable.
- !: The port is unreachable.
- !P: The protocol type is incorrect.
- !F: The packet is incorrectly fragmented.
- !S: The source route is incorrect.

Precautions

To ensure that the router properly responds to a Tracert request initiated by a source device when the router is the destination device to be tested, you must run the **icmp port-unreachable send** command to enable the device to send ICMP port-unreachable packets.

Once **-r** is specified, the outputs of both the **tracert** and **ping** commands show information about nodes between the source and the destination. Differences between the outputs of the **tracert** and **ping** commands are as follows:

- If the **ping** command times out on a transit node, a timeout packet is returned and the command output displays no path information.
- If the **tracert** command times out on a transit node, the command output displays " * * * " indicating that the tracert times out on the node but the tracert is not interrupted.

Example

Tracert the gateways from the source host to the destination host with the IP address being 10.1.1.11.

```
<Huawei> tracert 10.1.1.11
traceroute to 10.1.1.11 (10.1.1.11), max hops: 30, packet length: 40, press CTRL_C to break
1 10.3.112.1   10 ms 10 ms 10 ms
2 10.32.216.1  19 ms 19 ms 19 ms
3 * * *
4 * * *
5 * * *
6 * * *
7 10.1.1.11   339 ms 279 ms 279 ms
```

 Copyright © Huawei Technologies Co., Ltd.

Table 21-87 Description of the tracert command output

Item	Description
traceroute to	Tracert to a destination IP address.
max hops	Maximum TTL value.
packet length	Length of a sent packet.
10.3.112.1 10 ms 10 ms 10 ms	The integer 1 indicates the first hop gateway. Each hop increments the hop count. By default, the maximum hop count is 30. "10.3.112.1" is the gateway address of the first hop. The IPv4 address following the serial number of each hop is the gateway address of the hop. "10 ms 10 ms 10 ms" indicates the difference between the time when the three UDP packets are sent and when corresponding ICMP Time Exceeded or ICMP Port Unreachable messages are received. By default, each hop sends three UDP probe packets.
* * *	No ICMP Time Exceeded message or ICMP Port Unreachable message is returned within a specified period on the Nth hop. By default, an ICMP Time Exceeded message or ICMP Port-unreachable message should be returned within 5000 ms.

Related Topics

21.15.1 ping
21.15.2 ping ipv6
21.15.4 tracert ipv6

21.15.4 tracert ipv6

Function

The **tracert ipv6** command checks the path of packets from the source to the destination, checks IPv6 network connectivity, and locates a network fault.

Format

tracert ipv6 [**-a** *source-ipv6-address* | **-f** *first-hop-limit* | **-m** *max-hop-limit* | **-name** | **-p** *port-number* | **-q** *probes* | **-s** *packetsize* | **-w** *timeout* | **vpn-instance** *vpn-instance-name*] * *host*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
-a *source-ipv6-address*	Specifies the source address of a tracert packet. If this parameter is not specified, the IP address of the outbound interface is used as the source IP address for sending tracert packets.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
-f *first-hop-limit*	Specifies the initial hop-limit. Carried in the IPv6 header, the hop-limit (time to live) indicates the lifetime of IPv6 packets and specifies the maximum number of hops that the IPv6 packets can pass through. The hop-limit field in IPv6 packets is similar to the TTL field in the IPv4 packets. The hop-limit value is set on the source and reduced by 1 each time the packet passes through a Layer 3 device. When the hop-limit value is reduced to 0 on a Layer 3 device, the Layer 3 device discards the packet and sends an ICMPv6 Timeout message to the source. If *first-hop-limit* is specified and the number of hops is smaller than the specified value, the hop-limit value will be greater than 0 after the packet passes through all the nodes. Therefore, no ICMPv6 Timeout message is sent to the source. If *max-hop-limit* is specified, the value of *first-hop-limit* must be smaller than the value of *max-hop-limit*.	The value is an integer that ranges from 1 to 255. The default value is 1.
-m *max-hop-limit*	Specifies the maximum hop-limit. Usually, the maximum hop-limit is set to the number of hops that a packet passes through. To change the hop-limit value, you need to use this parameter. If *first-hop-limit* is specified, the value of *max-hop-limit* must be greater than the value of *first-hop-limit*.	The value is an integer that ranges from 1 to 255. The default value is 30.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-name	Displays the name of the destination host.	-
-p *port-number*	Specifies the UDP port number of the destination. • If no UDP port number is specified for the destination, when you run the **tracert ipv6** command, a port with the port number greater than 32768 is randomly chosen for the destination to receive tracert packets. • Before specifying the UDP port number for the destination, ensure that the port is not in use; otherwise, the tracert fails.	The value is an integer that ranges from 1 to 65535. The default value is 33434.
-q *probes*	Specifies the number of tracert packets sent each time. In the case of poor network quality, you can set *probes* to a comparatively large value to ensure that tracert packets can reach the destination.	The value is an integer that ranges from 1 to 65535. The default value is 3.
-s *packetsize*	Specifies the length of an ICMPv6 Echo Request message, excluding the IP header and ICMPv6 header.	The value is an integer that ranges from 20 to 9600, in bytes. The default value is 56.
-w *timeout*	Sets the timeout period to wait for a reply. If a tracert packet times out when reaching a gateway, an asterisk (*) is displayed. In the case of poor network quality and a low network transmission rate, you are advised to prolong the timeout period.	The value is an integer that ranges from 1 to 65535, in milliseconds. The default value is 5000.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance for the IPv6 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
host	Specifies the host name or IPv6 address of the destination host.	The value is a string of 1 to 255 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. The IPv6 address is a 32–bit string in hexadecimal format, namely, the format X:X:X:X:X:X:X:X.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

When a fault occurs on the network and the peer is an IPv6 device, you can run the **ping ipv6** command to check network connectivity based on the reply message, and then run the **tracert ipv6** command to locate the fault.

You can specify different parameters in the **tracert ipv6** command for different scenarios:

- To check information about nodes between the source and the IPv6 destination, run the **tracert ipv6** *host* command.
- To check information about nodes between the source and the IPv6 destination on a Layer 3 VPN, run the **tracert ipv6 vpn-instance** *vpn-instance-name host* command. On a Layer 3 VPN, devices may not have routing information about each other. Therefore, you cannot use the **tracert ipv6** *host* command to check whether the peer is reachable. To check information about nodes between the source and the IPv6 destination in a specified VPN instance, run the **tracert ipv6 vpn-instance** *vpn-instance-name host* command.
- On an unstable network, you can run the **tracert ipv6 -q** *probes* **-w** *timeout host* command to check information about nodes between the source and the IPv6 destination. If the network is unreliable, set the packet transmission count (**-q**) and timeout (**-w**) to the upper limits. This makes the test result accurate.
- To check information about nodes along a segment of a path, run the **tracert ipv6 -f** *first-hop-limit* **-m** *max-hop-limit host* command that has initial hop-limit and maximum hop-limit specified.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

- The UDP module of each node is working properly; otherwise, the IPv6 tracert operation fails.
- The VPN module of each node is working properly if **vpn-instance** is specified.
- The ICMPv6 module of each node is working properly; otherwise, " * * * " is displayed.

Procedure

The execution process of the **tracert ipv6** command is as follows:

- The source sends a packet with the hop-limit being 1. After the hop-limit times out, the first hop sends an ICMPv6 Error message to the source, indicating that the packet cannot be forwarded.
- The source sends a packet with the hop-limit being 2. After the hop-limit times out, the second hop sends an ICMPv6 Error message to the source, indicating that the packet cannot be forwarded.
- The source sends a packet with the hop-limit being 3. After the hop-limit times out, the third hop sends an ICMPv6 Error message to the source, indicating that the packet cannot be forwarded.
- The preceding process proceeds until the packet reaches the destination.

When receiving an IPv6 packet, each destination hop cannot find the port specified in the IPv6 packet, and therefore returns an ICMPv6 Port Unreachable message, indicating that the destination port is unreachable and the IPv6 tracert ends. In this manner, the result of each probe is displayed on the source, according to which you can find the path from the source to the destination.

Configuration Impact

If a fault occurs when you run the **tracert ipv6** command, the following information may be displayed:

- !H: The host is unreachable.
- !N: The network is unreachable.
- !: The port is unreachable.
- !P: The protocol type is incorrect.
- !F: The packet is incorrectly fragmented.
- !S: The source route is incorrect.

Precautions

By default, the ICMPv6 module is automatically enabled after you enable the IPv6 module.

Example

Set the number of packets to be sent to 5 and timeout period to 8000 ms, and tracert the gateways from the source to the destination at FC00::3.

```
<Huawei> tracert ipv6 -q 5 -w 8000 FC00::3
traceroute to FC00::3 30 hops max,60 bytes packet
1 FC00:1::3 26 ms 23 ms 26 ms 30 ms 29 ms
2 FC00::3 3020 ms 3024 ms 4040 ms 6820 ms 5584 ms
```

 Copyright © Huawei Technologies Co., Ltd.

Table 21-88 Description of the tracert ipv6 command output

Item	Description
traceroute to HH:HH::HH:H	IPv6 address of the destination host.
x hops max	Maximum hop-limit value.
x bytes packet	Length of a tracert packet.
1 2	Sequence number of the received ICMPv6 Echo Reply message.
HH:HH::HH:H	Address of the IPCMPv6 Echo Reply message.
26 ms 23 ms 26 ms	RTT, in milliseconds.

Related Topics

21.15.2 ping ipv6

Copyright © Huawei Technologies Co., Ltd.