16 Network Management and Monitoring Commands

16.1 SNMP Configuration Commands
16.2 RMON and RMON2 Configuration Commands
16.3 LLDP Configuration Commands
16.4 Performance Management Commands
16.5 iPCA Configuration Commands
16.6 iPCA 2.0 Configuration Commands
16.7 NQA Configuration Commands
16.8 Service Diagnosis Configuration Commands
16.9 Mirroring Configuration Commands
16.10 Packet Capture Configuration Commands
16.11 NetStream Configuration Commands
16.12 sFlow Configuration Commands
16.13 Ping and Tracert Configuration Commands
16.14 TWAMP Light Configuration Commands
16.15 NETCONF Configuration Commands
16.16 O&M information reporting Configuration Commands
16.17 eMDI Configuration Commands

16.1 SNMP Configuration Commands

16.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.1.2 bulk-file

Function

The **bulk-file** command creates a bulk file for bulk statistics collection and displays the bulk file view. If the specified bulk file exists, the command displays the bulk file view directly.

The **undo bulk-file** command deletes a bulk file.

By default, no bulk file is configured in the system.

Format

bulk-file *file-name*

undo bulk-file *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the name of a bulk file.	The value is a string of 1 to 31 characters. It can only contain digits, letters, underscores (_), and hyphens (-).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before creating a bulk file, run the **bulk-stat enable** command to enable bulk statistics collection.

Before deleting a bulk file, ensure that the bulk file exists and the bulk statistics collection task has been stopped. If the bulk file does not exist or the bulk statistics collection task is still running, the system displays an error message.

Example

Create a bulk file named **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
```



```
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable]
```

16.1.3 bulk-stat enable

Function

The **bulk-stat enable** command enables the bulk statistics collection function.

The **undo bulk-stat enable** command disables the bulk statistics collection function.

By default, the bulk statistics collection function is disabled.

Format

bulk-stat enable

undo bulk-stat enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable the system to collect statistics about multiple objects on the local device, generate a statistics file, and send the file to the NMS through FTP or TFTP, use the **bulk-stat enable** command to enable the bulk statistics collection function.

When disabling the bulk statistics collection function, you need to confirm your action in interactive mode.

Example

Enable the bulk statistics collection function.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
```

Disable the bulk statistics collection function.

```
<HUAWEI> system-view
[HUAWEI] undo bulk-stat enable
Warning: All bulk stat configuration will be deleted. Continue? [Y/N]:y
```


16.1.4 clear configuration snmp-agent trap enable

Function

The **clear configuration snmp-agent trap enable** command deletes alarm configurations related to one or all functions in a batch and restores the default alarm functions.

Format

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

Parameters

Parameter	Description	Value
feature-name *feature-name*	Deletes configurations of the trap function of a feature.	The value is the name of a feature that has been supported by the device.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a feature trap function is enabled or disabled using the **snmp-agent trap enable feature-name** *feature-name* [**trap-name** *trap-name*] command, the trap functions of all features are enabled using the **snmp-agent trap enable** command, or the trap functions of all features are disabled using the **snmp-agent trap disable** command. To delete the configurations, run the **clear configuration snmp-agent trap enable** command.

Configuration Impact

- When the trap function is enabled or disabled globally, running the **clear configuration snmp-agent trap enable feature-name** *feature-name* command deletes configurations of the trap function of the feature specified by *feature-name* and restores the status of the trap function to be the same as that of the global trap function.
- When the global trap function is in the default state, running the **clear configuration snmp-agent trap enable feature-name** *feature-name* command deletes configurations of the trap function of the feature specified by *feature-name* and restores the status of the trap function to be the default status.

- Running the **clear configuration snmp-agent trap enable** command deletes configurations of the trap functions of all features and restores all feature alarm functions to the default status.

Example

Delete configurations of the trap functions of all features.

```
<HUAWEI> system-view
[HUAWEI] clear configuration snmp-agent trap enable
```

16.1.5 collect enable

Function

The **collect enable** command enables an existing bulk file.

The **undo collect enable** command disables an existing bulk file.

By default, no bulk file is enabled.

Format

collect enable

undo collect enable

Parameters

None

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a bulk file is created, it is in Stop state and does not participate in data collection and scheduling. After you run the **collect enable** command to enable the bulk file, the bulk file transitions to Ready state and can participate in data collection and scheduling. The **undo collect enable** command disables the bulk file and sets the file state to Stop.

Precautions

Before running the **collect enable** command in a bulk file, run the **transfer** command to configure the primary upload path for the bulk file.

The interval between running the **undo collect enable** and **collect enable** commands in a bulk file must be at least 10 seconds. If the interval is less than 10 seconds, the **collect enable** configuration files.

You can change the maximum number of retransmissions, collection interval, upload interval, and upload holding time, and delete the primary URL for a bulk file only when the bulk file is disabled.

The **collect enable** command takes effect only when the collection interval, upload interval, and upload holding time meet the following requirements: The upload interval is an integral multiple of the collection interval, and the upload holding time is smaller than or equal to the upload interval.

Example

Enable the bulk file **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] transfer primary protocol ftp username user password pwd host 10 path folder/bulkstat1
[HUAWEI-bulk-file-iftable] collect enable
```

16.1.6 collect interval

Function

The **collect interval** command sets the statistics collection interval for a bulk file.

The **undo collect interval** command restores the default statistics collection interval.

By default, the statistics collection interval is 5 minutes.

Format

collect interval *interval*

undo collect interval

Parameters

Parameter	Description	Value
interval	Specifies statistics collection interval of a bulk file.	The value can be 5, 10, 15, or 30, in minutes.

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

The file upload interval configured using the **transfer interval** command must be an integral multiple of the statistics collection interval configured using this command.

Before changing the statistics collection interval, run the **undo collect enable** command to disable the statistics collection function.

Example

Set the statistics collection interval to 10 minutes for the bulk file **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] collect interval 10
```

16.1.7 display bulk-stat

Function

The **display bulk-stat** command displays the configuration of the bulk statistics collection function.

Format

display bulk-stat [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name of a bulk file.	The value is a string of 1 to 31 characters. It can only contain digits, letters, underscores (_), and hyphens (-).

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display bulk-stat** command displays the configuration of the bulk statistics collection function, including:

- Maximum number of bulk files
- Number of configured bulk files

- Maximum number of instances that can be collected within 5 minutes
- Basic configurations and status of configured bulk files

The **display bulk-stat** *file-name* command displays detailed information about the bulk file with the specified file name, including:

- File name, storage mode, and format of the bulk file
- Statistics collection interval and upload interval of the bulk file
- The primary URL and secondary URL where the bulk file will be uploaded
- Maximum number of retransmissions of the bulk file
- Storage time of the bulk file
- Current status of the bulk file
- Objects included in the bulk file

Example

Display the configuration of the bulk statistics collection function.

```
<HUAWEI> display bulk-stat
bulk statistic info:
--------------------------------
max bulk file number : 10
current bulk file number: 10
current bulk object number: 2000
max data item per 5 minutes: 40000
--------------------------------
index  bulk file name          collect(min)  transfer(min) status
-------------------------------------------------------------------------------------------------------------
 1     bulk1                   5             5             running
 2     bulk2                   5             15            ready
 3     bulk3                   5             10            stop
 4     bulk4                   5             15            ready
-------------------------------------------------------------------------------------------------------------
```

Table 16-1 Description of the **display bulk-stat** command output

Item	Description
max bulk file number	Maximum number of bulk files.
current bulk file number	Number of configured bulk files.
current bulk object number	Number of configured statistics objects.
max data item per 5 minutes	Maximum number of instances that can be collected within 5 minutes.
index	Index of a configured bulk file.
bulk file name	Name of a configured bulk file. You can run the **bulk-file** command to configure this parameter.
collect(min)	Statistics collection interval of a configured bulk file. You can run the **collect interval** command to configure this parameter.

Item	Description
transfer(min)	Upload interval of a configured bulk file. You can run the **transfer interval** command to configure this parameter.
status	Status of a configured bulk file. The value can be: • ready: The bulk file is ready for batch performance statistics collection. • running: The system is collecting performance statistics and writing data in the bulk file. • stop: The system has finished collecting performance statistics in the current collection interval.

Display detailed information about bulk file **iftable**.

```
<HUAWEI> display bulk-stat iftable
bulk file iftable:
--------------------------------
storage: ephemeral
format: bulkASCII
collect interval: 5 min
transfer interval: 15 min
primary transfer URL: sftp://user:password@host/folder/bulkstat1
secondary transfer URL: sftp://10.1.0.1/tftpboot/user/bulkstat1
transfer retry times: 3
file remain time: 15 min
status: running
last transfer success time: 2006-11-29 11:15
last transfer fail time: NULL
total object number: 2
--------------------------------
index: 1
class: single
OID: 1.3.6.1.2.1.10.94.1.1.10.1.1.0.1
start index: NULL
instance number: NULL
--------------------------------
index: 2
class: column
OID:  1.3.6.1.2.1.10.94.1.1.10.1.2
start index: 1
instance number: 3
```

Table 16-2 Description of the **display bulk-stat iftable** command output

Item	Description
storage	Storage mode of the bulk file. Currently, only the ephemeral storage mode is supported.
format	Format of the bulk file.

Item	Description
collect interval	Statistics collection interval of the bulk file. You can run the **collect interval** command to configure this parameter.
transfer interval	Upload interval of the bulk file. You can run the **transfer interval** command to configure this parameter.
transfer retry times	Maximum number of retransmissions of the bulk file. You can run the **transfer retry** command to configure this parameter.
primary transfer URL	Primary URL where the bulk file will be uploaded. You can run the **transfer** command to configure this parameter.
secondary transfer URL	Secondary URL where the bulk file will be uploaded. You can run the **transfer** command to configure this parameter.
file remain time	Storage time of the bulk file. You can run the **transfer remain-time** command to configure this parameter.
last transfer success time	Time of the last file upload success.
last transfer fail time	Time of the last file upload failure.
total object number	Total number of objects in the bulk file.
index	Index of an object.
class	Type of an object. The value can be: ● single: a single statistics object ● column: bulk statistics object
OID	OID of an object.
start index	● When the value of **class** is **single**, the parameter is displayed **NULL**. ● When the value of **class** is **column**, this parameter indicates the start instance index. You can run the **object** command to configure this parameter.

Item	Description
instance number	• When the value of **class** is **single**, the parameter is displayed **NULL**. • When the value of **class** is **column**, this parameter indicates the number of consecutive instances collected from the start instance index. You can run the **object** command to configure this parameter.

16.1.8 display snmp dynamic-control threshold

Function

The **display snmp dynamic-control threshold** command displays the CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks.

Format

display snmp dynamic-control threshold

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The **set snmp dynamic-control threshold** command is used to configure the CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks. The **display snmp dynamic-control threshold** command is used to check the current CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks.

Example

Check the current CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks.

```
<HUAWEI> display snmp dynamic-control threshold
Info: The current CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks is 60%.
```


Table 16-3 Description of the **display snmp dynamic-control threshold** command output

Item	Description
The current CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks is *threshold*.	When the CPU usage reaches the value specified by *threshold*, the device reduces resources for scheduling SNMP tasks.

16.1.9 display snmp-agent

Function

The **display snmp-agent** command displays the engine ID of the local or remote SNMP agent.

Format

display snmp-agent { **local-engineid** | **remote-engineid** }

Parameters

Parameter	Description	Value
local-engineid	Displays the engine ID of the local SNMP agent.	-
remote-engineid	Displays the engine ID of a remote SNMP agent.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the SNMP agent function is enabled, you can run the **display snmp-agent** { **local-engineid** | **remote-engineid** } command to view the engine ID of the local or remote SNMP agent.

The engine ID of the SNMP agent uniquely identifies an SNMP agent in a management domain. The engine ID of the SNMP agent is an important component of the SNMP agent. It schedules and processes SNMP messages, implements security authentication, access control and so on.

Prerequisites

Before running the **display snmp-agent** { **local-engineid** | **remote-engineid** } command to view the engine ID of the local or remote SNMP agent, you need to run the **snmp-agent** command to enable the SNMP agent function.

Precautions

To configure an engine ID for the local SNMP agent, you can run the **snmp-agent local-engineid** command.

Example

Display the engine ID of the local SNMP agent.

```
<HUAWEI> display snmp-agent local-engineid
  SNMP local EngineID: 800007DB03360102101100
```

Table 16-4 Description of the **display snmp-agent local-engineid** command output

Item	Description
SNMP local EngineID	The engine ID of the local SNMP agent.

16.1.10 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 community with read-only permission.	-
write	Displays the name of a community with read and write permission.	-

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.

If the parameter **read** or **write** is not specified, the names of all communities are displayed.

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
  Community name: %^%#.T|&Whvyf$<Gd"I,wXi5SP_6~Nakk6<<+3H:N-h@aJ6d,l0md%HCeAY8~>X=>xV
\JKNAL=124r839v<*%^%#
      Group name: %^%#.T|&Whvyf$<Gd"I,wXi5SP_6~Nakk6<<+3H:N-h@aJ6d,l0md%HCeAY8~>X=>xV
\JKNAL=124r839v<*%^%#
      Alias name:huawei
      Acl:2001
      Storage type: nonVolatile
```

Table 16-5 Description of the **display snmp-agent community** command output

Item	Description
Community name	Name of a community.
Group name	Name of a group.
Alias name	Alias name for a community
Acl	The ACL takes effect on both IPv4 and IPv6 networks.
Ipv4 acl	The ACL takes effect on only IPv4 network.
Ipv6 acl	The ACL takes effect on only IPv6 network.
Storage type	Mode in which information is stored. Only nonVolatile is supported currently. In this mode, configuration can be restored after the device restarts.

16.1.11 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 to the NMS is enabled on the device.

Example

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

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

Table 16-6 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 to the NMS is enabled on the device: • enabled: The function is enabled. • disabled: The function is disabled. You can run the **snmp-agent extend error-code enable** command to configure this parameter.

16.1.12 display snmp-agent group

Function

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

Format

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

Parameters

Parameter	Description	Value
group-name	Displays information about a specified SNMP user group. If this parameter is not specified, the system displays information about all SNMP user groups.	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 SNMP user group, you can run the **display snmp-agent group** command to view information about the SNMP user group, such as the group name and security model.

Prerequisites

An SNMP user group has been configured using the **snmp-agent group** command.

Example

Display information about all SNMP user groups.

```
<HUAWEI> display snmp-agent group
  Group name: testgroup
     Security model: v3 AuthPriv
     Readview: ViewDefault
     Writeview: dnsmib
     Notifyview: dnsmib
     Storage type: nonVolatile
     Acl: 2001
```


Table 16-7 Description of the **display snmp-agent group** command output

Item	Description
Group name	Name of the SNMP user group.
Security model	Security mode of the SNMP user group: • v3 AuthPriv: SNMP packets need to be authenticated and encrypted. • v3 AuthnoPriv: SNMP packets only need to be authenticated. • v3 noAuthnoPriv: SNMP packets neither need to be authenticated nor encrypted.
Readview	Name of a MIB view with read-only permission of the SNMP user group.
Writeview	Name of a MIB view with read and write permission of the SNMP user group.
Notifyview	Name of a MIB view name with notification permission of the SNMP user group.
Storage-type	Mode in which information is stored. Only nonVolatile is supported currently. In this mode, configuration can be restored after the device restarts.
Acl	The ACL takes effect on both IPv4 and IPv6 networks.
Ipv4 acl	The ACL takes effect on only IPv4 network.
Ipv6 acl	The ACL takes effect on only IPv6 network.

16.1.13 display snmp-agent heartbeat configuration

Function

The **display snmp-agent heartbeat configuration** command displays the configuration of sending heartbeat packets to the NMS.

Format

display snmp-agent heartbeat configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the NMS cannot initiatively obtain the status of the device, run the **snmp-agent heartbeat enable** command to enable the device to send heartbeat packets to the NMS. The device then periodically sends heartbeat packets to the NMS to notify the NMS of its status. To check whether the device is enabled to send heartbeat packets to the NMS, run the **display snmp-agent heartbeat configuration** command.

Example

Display the configuration of sending heartbeat packets to the NMS.

```
<HUAWEI> display snmp-agent heartbeat configuration
SNMP agent heartbeat configuration:
 Status   :    Enabled
 Interval :    60(s)
```

Table 16-8 Description of the **display snmp-agent heartbeat configuration** command output

Item	Description
SNMP agent heartbeat configuration	Configuration of sending heartbeat packets to the NMS.
Status	Whether the device is enabled to send heartbeat packets to the NMS: • Enabled: The function is enabled. • Disabled: The function is disabled. You can run the **snmp-agent heartbeat enable** command to configure this parameter.
Interval	The interval at which the device sends heartbeat packets to the NMS. You can run the **snmp-agent heartbeat interval** command to configure this parameter.

16.1.14 display snmp-agent inform

Function

The **display snmp-agent inform** command displays parameters for sending traps to the NMS through Inform packets and statistics about the Inform packets.

Format

display snmp-agent inform [**address udp-domain** *ip-address* [**vpn-instance** *vpn-instance-name*] **params securityname** { *security-name* | **cipher** *security-name* }]

Parameters

Parameter	Description	Value
address udp-domain *ip-address*	Specifies the IP address of the NMS, with the transmission domain of the target host being based on the User Datagram Protocol (UDP). **NOTE** The IP address specified by **address** and the security name specified by **securityname** together identify an NMS.	The value is dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the VPN instance to which the NMS belongs. **NOTE** On the VPN, the VPN instance specified by **vpn-instance**, IP address, and security name together identify an NMS.	The value must be an existing VPN instance name.
params	Indicates information about the NMS.	-
securityname *security-name*	Specifies the user security name displayed on the NMS.	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.

Parameter	Description	Value
cipher *security-name*	Indicates the unencrypted or encrypted string of security name.	The value is a string of 1 to 32 case-sensitive characters or a string of 32 or 56 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. ● When the community name is a string of 1 to 32 characters, the string is processed as plain text by default and will be encrypted. ● When the community name is a string of 32 or 56 characters, the string is processed as cipher text by default, and the system will determine whether the string can be parsed.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display snmp-agent inform** command displays parameters for sending traps to the NMS through Inform packets and statistics about the Inform packets:

- Number of times Inform packets are retransmitted when the device receives no acknowledgement message from the NMS.
- Timeout period for the acknowledgement from the NMS in response to Inform packets.
- Number of Inform packets retransmitted to the NMS.
- Number of Inform packets in the Inform buffer to be acknowledged by the NMS.
- Number of traps sent through Inform packets to the NMS.
- Number of Inform packets discarded when the Inform buffer is full.
- Number of retransmitted Inform packets that are not acknowledged.
- Number of packets acknowledged by the NMS.

If no parameter is specified in the **display snmp-agent inform** command, global parameters for sending traps through Inform packets, all NMS parameters, and packet statistics mode are displayed.

Example

Displays global parameters for sending traps through Inform packets, all NMS parameters, and packets statistics mode.

```
<HUAWEI> display snmp-agent inform
Global config: resend-times 3, timeout 15s, pending 39
Global status: current notification count 1
Target-host ID: VPN instance/IP-Address/Domain/Security name
-/10.1.1.1/-/%^%#O>tf1ssv|~v3.\IY}|@Gk,:%/IX{!OrFazE#1lxR%^%#:
   Config: resend-times 3, timeout 15s
   Status: retries 0, pending 0, sent 0, dropped 0, failed 0, confirmed 0
```

Table 16-9 Description of the **display snmp-agent inform** command output

Item	Description
Global config	Global Inform parameters: • resend-times: indicates the number of times Inform packets are retransmitted when the device receives no acknowledgement message from the NMS. • timeout: indicates timeout period for the acknowledgement from the NMS in response to Inform packets, in seconds. • pending: indicates the number of Inform packets in the Inform buffer to be acknowledged by the NMS. You can run the **snmp-agent inform** command to configure these parameters.
Global status	Statistics about global Inform packets.
Target-host ID: VPN instance/IP-Address/ Domain/Security name	You can run the **snmp-agent inform address** command to configure these parameters (except Domain).
Config	Inform packet parameters of the NMS: • resend-times: indicates the number of times Inform packets are retransmitted when the device receives no acknowledgement message from the NMS. • timeout: Indicates timeout period for the acknowledgement from the NMS in response to Inform packets. You can run the **snmp-agent inform address** command to configure these parameters.

Item	Description
Status	Statistics about Inform packets from the switch to the NMS: • retries: Number of Inform packets retransmitted to the NMS. • pending: indicates the number of Inform packets in the Inform buffer to be acknowledged by the NMS. • sent: Number of traps sent through Inform packets to the NMS. • dropped: Number of Inform packets discarded when the Inform buffer is full. • failed: Number of retransmitted Inform packets that are not acknowledged. • confirmed: Number of packets acknowledged by the NMS.

16.1.15 display snmp-agent mib-view

Function

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

Format

display snmp-agent mib-view [**exclude** | **include** | **viewname** *view-name*]

Parameters

Parameter	Description	Value
exclude	Displays all MIB views that have excluded MIB subtrees configured.	-
include	Displays all MIB views that have included MIB subtrees configured.	-
viewname *view-name*	Displays a specified MIB 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.

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 current MIB view, you can run the **display snmp-agent mib-view** command.

Precautions

The **snmp-agent** command has been run to enable the SNMP Agent. Otherwise, an error message is displayed.

Example

Display the current MIB view.

```
<HUAWEI> display snmp-agent mib-view
  View name:ViewDefault
    MIB Subtree:internet
    Subtree mask:F0(Hex)
    Storage-type: nonVolatile
    View Type:included
    View status:active
```

Table 16-10 Description of the **display snmp-agent mib-view** command output

Item	Description
View name	MIB view name. You can run the **snmp-agent mib-view** command to configure this parameter.
MIB Subtree	MIB subtree. You can run the **snmp-agent mib-view** command to configure this parameter.
Subtree mask	MIB subtree mask.
Storage type	Mode in which information is stored. Only nonVolatile is supported currently. In this mode, configuration can be restored after the device restarts.

Item	Description
View Type	Whether the MIB subtree can be accessed by a MIB view: • included: The MIB subtree can be accessed by a MIB view. • excluded: The MIB subtree cannot be accessed by a MIB view. You can run the **snmp-agent mib-view** command to configure this parameter.
View status	Indicates the status of the MIB view.

16.1.16 display snmp-agent notification-log

Function

The **display snmp-agent notification-log** command displays information saved in the trap log buffer.

Format

display snmp-agent notification-log [**info** | **logtime** *starttime* **to** *endtime* | **size** *size*]

Parameters

Parameter	Description	Value
info	Displays parameters of trap logs recorded by the device and statistics about trap logs.	-
logtime *starttime* **to** *endtime*	Specifies the start time and end time of trap logs to be displayed: • *starttime*: specifies the start time of trap logs. • *endtime*: specifies the end time of trap logs.	The value is in the HH:MM:SS YYYY/MM/DD format, where HH:MM:SS indicates the hour, minute, and second and YYYY/MM/DD indicates the year, month, and day. HH ranges from 0 to 23; MM and SS range from 0 to 59. YYYY ranges from 2000 to 2099; MM ranges from 1 to 12; DD ranges from 1 to 31. The end time must be later than the start time.

Parameter	Description	Value
size *size*	Specifies the number of latest trap logs to be displayed.	The value is an integer that ranges from 1 to 5000.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use any of the following methods to view logs in the trap log buffer using the **display snmp-agent notification-log** command:

- Specify the start time and end time of trap logs to be displayed.
- Specify the number of latest trap logs to be displayed.
- Specify no parameter to view all trap logs.

Example

Display parameters of trap logs recorded by the device and statistics about trap logs.

```
<HUAWEI> display snmp-agent notification-log info
Notification log information :
Notification Admin Status: enable
GlobalNotificationsLogged: 0
GlobalNotificationsBumped: 0
GlobalNotificationsLimit: 500
GlobalNotificationsAgeout: 24
Total number of notification log(s): 0
```

Table 16-11 Description of the **display snmp-agent notification-log info** command output

Item	Description
Notification log information	Parameters of trap logs recorded by the device and statistics about trap logs.
Notification Admin Status	Whether the function of recording trap logs is enabled on the device: • enable: The function is enabled. • disable: The function is disabled. You can run the **snmp-agent notification-log enable** command to configure this parameter.
GlobalNotificationsLogged	Number of trap logs recorded currently.

Item	Description
GlobalNotificationsBumped	Number of logs recording discarded traps.
GlobalNotificationsLimit	Maximum number of trap logs that can be saved. You can run the **snmp-agent notification-log** command to configure this parameter.
GlobalNotificationsAgeout	Aging time of trap logs. You can run the **snmp-agent notification-log** command to configure this parameter.
Total number of notification log(s)	Total number of recorded trap logs.

Display the latest 20 trap logs. (In this example, only one trap log is available in the system.)

```
<HUAWEI> display snmp-agent notification-log size 20
 Total number of notifications log(s) : 1

LogTable :
  LogIndex= 12
  LogTime= 229323
  LogDateAndTime= 2007/3/8 10:28:16
  LogEngineID= 000007DB7F00000100004CFB
  LogEngineTAddress= 192.168.39.1/162
  LogEngineTDomain= snmpUDPDomain
  LogContextEngineID= null
  LogContextName= null
  LogNotificationID= 1.3.6.1.4.1.2011.6.10.2.1
LogVariableTable :
  LogVariableIndex= 1
  LogVariableOID= 1.3.6.1.2.1.1.3
  LogVariableValueType= TimeTicksLogVariableValue = 229323
  LogVariableIndex= 2
  LogVariableOID= 1.3.6.1.6.3.1.1.4.1
  LogVariableValueType= OidLogVariableValue = 1
  LogVariableIndex= 3
  LogVariableOID= 1.3.6.1.4.1.2011.6.10.1.1.7.1.3.29
  LogVariableValueType= Integer32LogVariableValue = 1
  LogVariableIndex= 4
  LogVariableOID= 1.3.6.1.4.1.2011.6.10.1.1.7.1.4.29
  LogVariableValueType= Integer32LogVariableValue = 3
  LogVariableIndex= 5
  LogVariableOID= 1.3.6.1.4.1.2011.6.10.1.1.7.1.5.29
  LogVariableValueType= Integer32LogVariableValue = 2
```

Table 16-12 Description of the **display snmp-agent notification-log size 20** command output

Item	Description
LogTable	Log table.
LogIndex	Index of the log.

Item	Description
LogTime	Difference between the time when the log was recorded and the time when the system started. The unit is 10 ms.
LogDateAndTime	Absolute date and time when the log was recorded.
LogEngineID	Engine ID of the SNMP message recorded in the log.
LogEngineTAddress	IP address and port number of the SNMP message recorded in the log.
LogEngineTDomain	Transmission type of the SNMP message recorded in the log.
LogContextEngineID	Engine ID of context of the SNMP message recorded in the log.
LogContextName	Secure user name, IP address, and VPN instance name.
LogNotificationID	OID of the trap object recorded in the log.
LogVariableTable	Variable table of the log.
LogVariableIndex	Index of a variable.
LogVariableOID	OID of a variable.
LogVariableValueType	Value type of a variable.
LogVariableValue	Value of a variable.

16.1.17 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 [*profile-name*]

Parameters

Parameter	Description	Value
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.

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
  Notify-filter name:snmpv2
  Notify-filter Subtree:snmpV2
  Notify-filter Subtree mask:F8(Hex)
  Notify-filter Storage-type:nonVolatile
  Notify-filter Type:included
  Notify-filter status:active
```

Table 16-13 Description of the **display snmp-agent notify-filter-profile** command output

Item	Description
Notify-filter name	Name of a trap filter profile. You can run the **snmp-agent notify-filter-profile** command to configure this parameter.
Notify-filter Subtree	Filtered MIB subtree. You can run the **snmp-agent notify-filter-profile** command to configure this parameter.
Notify-filter Subtree mask	Mask of a MIB subtree.

Item	Description
Notify-filter Storage-type	Mode in which information is stored. Only nonVolatile is supported currently. In this mode, configuration can be restored after the device restarts.
Notify-filter Type	Whether traps of the MIB subtree are sent to the NMS: • included: Traps of the MIB subtree are sent to the NMS. • excluded: Traps of the MIB subtree are not sent to the NMS. You can run the **snmp-agent notify-filter-profile** command to configure this parameter.
Notify-filter status	Status of a trap filter profile.

16.1.18 display snmp-agent statistics

Function

The **display snmp-agent statistics** command displays statistics about SNMP packets on the switch.

Format

display snmp-agent statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

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.

You can run the **display snmp-agent statistics** command to analyze the statistics about SNMP packets exchanged between the NMS and SNMP Agent, facilitating fault location.

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 SNMP packets on the switch.

```
<HUAWEI> display snmp-agent statistics
 0 Messages delivered to the SNMP entity
 0 Messages which were for an unsupported version
 0 Messages which used a SNMP community name not known
 0 Messages which represented an illegal operation for the community supplied
 0 ASN.1 or BER errors in the process of decoding
 7 Messages passed from the SNMP entity
 0 SNMP PDUs which had badValue error-status
 0 SNMP PDUs which had genErr error-status
 0 SNMP PDUs which had noSuchName error-status
 0 SNMP PDUs which had tooBig error-status
 0 MIB objects retrieved successfully
 0 MIB objects altered successfully
 0 GetRequest-PDU accepted and processed
 0 GetNextRequest-PDU accepted and processed
 0 GetResponse-PDU accepted and processed
 0 SetRequest-PDU accepted and processed
 0 Trap-PDU accepted and processed
 0 Inform-PDU sent
 0 Inform ACK PDUs failed to be processed
 0 Inform ACK PDUs successfully processed
```

Table 16-14 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 SNMP messages with version errors
Messages which used a SNMP community name not known	Number of SNMP messages with community name errors
Messages which represented an illegal operation for the community supplied	Number of SNMP messages with authority errors corresponding to community name
ASN.1 or BER errors in the process of decoding	Number of SNMP messages with encoding errors

Item	Description
Messages passed from the SNMP entity	Total number of sent SNMP messages
SNMP PDUs which had badValue error-status	Number of SNMP messages with bad values
SNMP PDUs which had genErr error-status	Number of SNMP messages with general errors
SNMP PDUs which had noSuchName error-status	Number of SNMP messages with requests for non-existing MIB objects
SNMP PDUs which had tooBig error-status	Number of SNMP messages with Too_big errors
MIB objects retrieved successfully	Number of variables requested by NMS
MIB objects altered successfully	Number of variables set by NMS
GetRequest-PDU accepted and processed	Number of received SNMP Get-request messages
GetNextRequest-PDU accepted and processed	Number of received SNMP GetNext-request messages
GetResponse-PDU accepted and processed	Number of sent SNMP Get-response messages
SetRequest-PDU accepted and processed	Number of received SNMP Set-request messages
Trap-PDU accepted and processed	Number of sent SNMP Trap messages
Inform-PDU sent	Number of sent SNMP Inform messages
Inform ACK PDUs failed to be processed	Number of SNMP Inform messages received with no acknowledgement
Inform ACK PDUs successfully processed	Number of SNMP Inform messages received with acknowledgement

16.1.19 display snmp-agent statistics mib

Function

The **display snmp-agent statistics mib** command displays statistics about the NMS's operations on MIB objects.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

display snmp-agent statistics mib [[**vpn-instance** *vpn-instance-name*] { **address** *ipv4-address* | **ipv6** *ipv6-address* }]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance name.	The value must be an existing VPN instance name.
address *ipv4-address*	Specifies an IPv4 address.	-
ipv6 *ipv6-address*	Specifies an IPv6 address.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An NMS performs operations on MIB objects to manage devices. To check these operation statistics, run the **display snmp-agent statistics mib** command. The command output displays names, access frequencies, and handling dates of MIB objects.

If no NMS is specified, the **display snmp-agent statistics mib** command displays statistics about the operations performed by all NMSs (that is, IPv4+VPN, IPv6+VPN, IPv4, and IPv6 NMSs) on MIB objects.

Follow-up Procedure

If the NMS accesses a great amount of MIB node information and statistics do not need to be saved, run the **reset snmp-agent statistics mib** command to delete the statistics.

Example

Display all statistics about the NMS's operations on MIB objects.


```
<HUAWEI> display snmp-agent statistics mib
-------------------------------------------------------------------------------
ip address:192.168.1.4, total mib node number:9
   SUMMARY:    Total set:0,Total get:9,Total get-next:75
-------------------------------------------------------------------------------
MibNode                    Set       Get       GetNext    MaxTime MinTime
AveTime

ifEntry                  0         0         75        0      0      0
ifNumber                   0         1         0         0      0      0
sysContact                 0         1         0         0      0      0
sysDescr                 0         1         0         0      0      0
sysLocation                0         1         0         0      0      0
sysName                    0         1         0         0      0      0
sysObjectID                0         1         0         0      0      0
sysServices              0         1         0         0      0      0
sysUpTime                  0         2         0         0      0      0
```

Display the statistics about the operations performed by the NMS with the IP address of 192.168.1.3 in the VPN instance **aa**.

```
<HUAWEI> display snmp-agent statistics mib vpn-instance aa address 192.168.1.3
-------------------------------------------------------------------------------
vpn instance:aa, ip address:192.168.1.3, total mib node number:
1
   SUMMARY:    Total set:0,Total get:1,Total get-next:0
-------------------------------------------------------------------------------
MibNode                    Set       Get       GetNext    MaxTime MinTime
AveTime

sysDescr                 0         1         0         0      0      0
```

Table 16-15 Description of the **display snmp-agent statistics mib** command output

Item	Description
ip address	IP address of the NMS.
vpn instance	VPN instance name
total mib node number	Total number of MIB objects accessed by the NMS.
SUMMARY	Abstract of statistics about the NMS's operations on MIB objects.
Total set	Total number of Set operations performed on all MIB objects.
Total get	Total number of Get operations performed on all MIB objects.
Total get-next	Total number of GetNext operations performed on all MIB objects.
MibNode	MIB object name.
Set	Number of the Set operations performed on a specified MIB object.
Get	Number of the Get operations performed on a specified MIB object.

Item	Description
GetNext	Number of the GetNext operations performed on a specified MIB object.
MaxTime	Maximum time for an operation performed on MIB objects, in milliseconds.
MinTime	Minimum time for an operation performed on MIB objects, in milliseconds.
AveTime	Average time for an operation performed on MIB objects, in milliseconds.

16.1.20 display snmp-agent sys-info

Function

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

Format

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

Parameters

Parameter	Description	Value
contact	Displays contact information of device maintenance personnel.	-
location	Displays the physical location of the device.	-
version	Displays the SNMP version running on the device.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display snmp-agent sys-info** command to display SNMP information about the device, including:

- Contact information of device maintenance personnel
- Physical location of the device
- SNMP version running on the device

If no parameter is specified, all information is displayed.

Example

Display all SNMP information about the device.

```
<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:
        Polling: SNMPv1:disable, SNMPv2c:disable,
SNMPv3:enable
        Trap   : SNMPv1:disable, SNMPv2c:enable,
SNMPv3:disable
```

Display the SNMP version running on the device.

```
<HUAWEI> display snmp-agent sys-info version
  SNMP version running in the system:
        Polling: SNMPv1:disable, SNMPv2c:disable,
SNMPv3:enable
        Trap   : SNMPv1:disable, SNMPv2c:enable,
SNMPv3:disable
```

Display contact information of device maintenance personnel.

```
<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 of the device.

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

Table 16-16 Description of the **display snmp-agent sys-info** command output

Item	Description
The contact person for this managed node	Contact information of device maintenance personnel, which is useful in event of emergencies. You can run the **snmp-agent sys-info** command to configure this parameter.
The physical location of this node	Physical location of the device. You can run the **snmp-agent sys-info** command to configure this parameter.

Item	Description
SNMP version running in the system	SNMP version running on the device. The value can be any combination of SNMPv1, SNMPv2c, and SNMPv3. When multiple versions are configured, the NMS manages the device using multiple SNMP versions. You can run the **snmp-agent sys-info** command to configure this parameter.
Polling	• SNMPv1: The function status is **enable** only when SNMPv1 is enabled and an SNMPv1 community name is configured. Otherwise, it is **disable**. • SNMPv2: The function status is **enable** only when SNMPv2 is enabled and an SNMPv2 community name is configured. Otherwise, it is **disable**. • SNMPv3: The function status is **enable** only when SNMPv3 is enabled and an SNMPv3 user name (excluding remote-engineid users) is configured. Otherwise, it is **disable**.
Trap	• SNMPv1: The trap host status is **enable** only when SNMPv1 is enabled and a trap host is configured. Otherwise, it is **disable**. • SNMPv2: The trap host status is **enable** only when SNMPv2 is enabled and a trap host is configured. Otherwise, it is **disable**. • SNMPv3: The trap host status is **enable** only when SNMPv3 is enabled and a trap host is configured. Otherwise, it is **disable**.

16.1.21 display snmp-agent target-host

Function

The **display snmp-agent target-host** command displays the configurations of destination hosts of all alarms.

Format

display snmp-agent target-host

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use the **display snmp-agent target-host** command to display the configurations of destination hosts of all traps, including IP addresses of the hosts, modes in which traps are sent, security name used to send traps, and SNMP versions. At present, the system can save the configuration of a maximum of 20 destination hosts. Therefore, the **display snmp-agent target-host** command can view the configuration of a maximum of 20 destination hosts.

Example

Display the configurations of destination hosts of all alarms.

```
<HUAWEI> display snmp-agent target-host
Target-host NO. 1
------------------------------------------------------------
 IP-address    : 10.1.2.1
 Domain        : -
 Source interface : -
 VPN instance  : -
 Security name : %^%#uq/!YZfvW4*vf[~C|.:Cl}UqS(vXd#wwqR~5M(rU%%^%#
 Port          : 162
 Type          : trap
 Version       : v2c
 Level         : No authentication and privacy
 NMS type      : HW NMS
 With ext-vb:  : No
------------------------------------------------------------
```

Table 16-17 Description of the **display snmp-agent target-host** command output

Parameter	Description
Target-host NO	Target host number, which is generated based on the sequence in which the target host is configured. You can run the **snmp-agent target-host inform** or **snmp-agent target-host trap** command to configure parameters of the target host.
IP-address	IP address of the target host.
Domain	Domain name of the target host.
Source interface	Source interface that sends traps.
VPN instance	VPN instance to which the target host belongs.
Security name	Security name used to send traps.
Port	UDP port number used to send traps.

Parameter	Description
Type	Mode in which traps are sent: • trap • inform
Version	SNMP version: • v1 • v2c • v3
Level	Security mode of packets: • Authentication: Packets only need to be authenticated. • Privacy: Packets need to be authenticated and encrypted. • No authentication and privacy: Packets need neither to be authenticated nor encrypted.
NMS type	Type of the target host: • NMS: indicates a network management system, which can be a Huawei NMS or an NMS from another vendor. • HW NMS: indicates a Huawei NMS. The traps sent to the Huawei NMS can contain more detailed information.
With ext-vb	Whether the trap sent to the target host carries extended bound variables: • No • Yes

16.1.22 display snmp-agent trap all

Function

The **display snmp-agent trap all** command displays whether the switch is enabled to send alarms of all features to the NM station.

Format

display snmp-agent trap all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display snmp-agent trap all** command to check whether the switch is enabled to send alarms of specified features to the NMS. You can configure this function by running **snmp-agent trap enable**, **snmp-agent trap enable feature-name**, and **snmp-agent trap disable**.

Example

Check whether the switch is enabled to send alarms of specified features to the NMS.

```
<HUAWEI> display snmp-agent trap all
------------------------------------------------------------------------------
Feature name: INFO
Trap number : 2
------------------------------------------------------------------------------
Trap name                     Default switch status   Current switch status
hwICLogFileAging                on                      on
hwICLogBufferLose               on                      on
------------------------------------------------------------------------------
---- More ----
```

Table 16-18 Description of the display snmp-agent trap all command output

Item	Description
Feature name	Name of the feature that generates alarms.
Trap number	Number of alarms generated by this feature.
Trap name	Name of the alarm.
Default switch status	Default status of the alarm: • on: The switch is enabled to send this alarm to the NMS. • off: The switch is disabled to send this alarm to the NMS.
Current switch status	Current status of the alarm: • on: The switch is enabled to send this alarm to the NMS. • off: The switch is disabled to send this alarm to the NMS. This status can be configured using the **snmp-agent trap enable feature-name** command.

16.1.23 display snmp-agent trap feature-name all

Function

The **display snmp-agent trap feature-name all** command displays whether the device is enabled to send alarms of specified features to the NMS.

Format

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

Parameters

Parameter	Description	Value
feature-name	Specifies the feature that generates alarms.	acle, adpvxlan, arp, asmngtrap, bfd, bgp, cfgmgr, clkm, configuration, datasync, dhcp, dldp, easyoperatrap, efm, emdi, entityexttrap, entitymib, entitytrap, eoam-1ag, eoam-y1731, erps, error-down, etrunk, fm, ftp_server, gtl, hgmp, hsb-trap, http, ifnet, ifpdt, igmp, info, ip, ipfpm, iplpm, ipsec, ipv6, isis, l2bptnl, l2if, l2ifppi, l2vpn, l3mb, l3vpn, lacp, lbdt, ldp, line, lldptrap, loopdetect, mad, mcast, mid_aaa, mid_am, mid_eapol, mid_web, mld, mpls, mpls_lspm, mpls_rsvp, mrm, msdp, mstp, ntp, ospf, ospfv3, pim, pim-std, pki, pm, ptp, qose, radius, rip, rm, rmon, rrpp, securitytrap, sindex, snmp, srmtrap, sspadp, stack, swithsrvres, sysres, system, tcp, trunk, tunnel-te, uni-topomng, uni-tplm, uni-vermng, unimbrtrap, usbloadtrap, vbst, vcmp, vfs, vplsoam, vrrp, wlan

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display snmp-agent trap feature-name all** command to check whether the switch is enabled to send alarms of specified features to the NMS. You can use the **snmp-agent trap enable feature-name** command to enable this function.

Precautions

- The feature name asmngtrap, uni-topomng, uni-tplm, uni-vermng, and unimbrtrap are supported only on the SVF parent.
- The feature name etrunk is supported only on the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.
- The feature name igmp, mld, mrm, msdp, pim-std, and pim are supported only on the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.
- The feature name gtl takes effect only on the device that loads the license control item.
- If the IS-IS trap function is enabled before a version upgrade, you need to run the **snmp-agent trap enable feature-name isis** command to re-enable the trap function after the version upgrade. Otherwise, the previous configuration is lost.

Example

Display the status of the ARP alarms.

```
<HUAWEI> display snmp-agent trap feature-name arp all
------------------------------------------------------------------------------
Feature name: ARP
Trap number : 4
------------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
hwEthernetARPSpeedLimitAlarm    on                      on
hwEthernetARPThresholdExceedAlarm
                               on                      on
hwEthernetARPThresholdResumeAlarm
                               on                      on
hwEthernetARPIPConflictEvent    on                      on
```

Table 16-19 Description of the display snmp-agent trap feature-name all command output

Item	Description
Feature name	Name of the feature that generates alarms.
Trap number	Number of alarms generated by this feature.
Trap name	Name of the alarm. For details about the alarm, see the Alarm Handling.
Default switch status	Default status of the alarm: • on: The switch is enabled to send this alarm to the NMS. • off: The switch is disabled to send this alarm to the NMS.

Item	Description
Current switch status	Current status of the alarm: • on: The switch is enabled to send this alarm to the NMS. • off: The switch is disabled to send this alarm to the NMS. This status can be configured using the **snmp-agent trap enable feature-name** command.

16.1.24 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 [**engineid** *engineid* | **group** *group-name* | **username** *user-name*] *

Parameters

Parameter	Description	Value
engineid *engineid*	Displays information about an SNMPv3 user with a specified SNMP entity engine ID.	-
group *group-name*	Displays the SNMPv3 user belonging to a specified user group.	-
username *user-name*	Displays information about a specified SNMPv3 user.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display snmp-agent usm-user** command to display the SNMPv3 user information configured through the **snmp-agent usm-user** command. The

SNMPv3 user here refers to the remote user that carries out SNMPv3 management. The displayed information about an SNMPv3 user includes the user name, authentication protocol, encryption algorithm, and user group to which the SNMPv3 user belongs.

Example

Display information about all current SNMPv3 users.

```
<HUAWEI> display snmp-agent usm-user
  User name: myuser01
     Engine ID: 800007DB03360102101100 active
     Authentication Protocol: sha2-256
     Privacy Protocol: aes256
     Group name: mygroup
     Ipv4 acl : 2000
     Ipv6 acl : 2004
<HUAWEI> display snmp-agent usm-user
  User name: myuser02
     Engine ID: 800007DB03360102101100 active
     Authentication Protocol: sha2-256
     Privacy Protocol: aes256
     Group name: mygroup
     Acl: 2000
```

Table 16-20 Description of the **display snmp-agent usm-user** command output

Item	Description
User name	SNMPv3 user name.
Engine ID	Local SNMP engine ID.
active	Status of the SNMPv3 user.
Authentication Protocol	Authentication algorithm used for the SNMPv3 user.
Privacy Protocol	Encryption algorithm used for the SNMPv3 user.
Group name	User group to which the SNMPv3 user belongs.
Acl	The ACL takes effect on both IPv4 and IPv6 networks.
Ipv4 acl	The ACL takes effect on only IPv4 network.
Ipv6 acl	The ACL takes effect on only IPv6 network.

16.1.25 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.

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

Disable an interface from sending a trap to the NMS when the protocol status of the interface changes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo enable snmp trap updown
```

16.1.26 format (bulk file view)

Function

The **format** command configures the format for a bulk file.

The **undo format** command restores the default format of a bulk file.

By default, the format of a bulk file is bulkascii (text format).

Format

format bulkascii

undo format

Parameters

Parameter	Description	Value
bulkascii	Indicates the text format.	-

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

Currently, the system supports only the text format of bulk files. The command can be upgraded to support more file formats, such as word and xml.

Example

Set the format of the bulk file **iftable** to bulkascii.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] format bulkascii
```

16.1.27 object

Function

The **object** command creates a statistics object for a bulk file.

The **undo object** command deletes a statistics object.

By default, no statistics object exists in a bulk file.

Format

object *oid* **class** { **single** | **column** [**start-index** *start-index*] [**instance-number** *instance-number*] }

undo object *oid* **class** { **single** | **column** }

Parameters

Parameter	Description	Value
oid	Specifies the OID of a statistics object. The value is a numeric string of 1 to 127 characters, in dotted notation.	-
class single	Creates a single statistics object.	-
class column	Creates a bulk statistics object.	-
start-index *start-index*	Specifies the start instance index when the object type is set to **column**. The value is a numeric string of 1 to 127 characters, in dotted notation. The value 0 indicates that the system collects statistics from the first instance in the column. The default value is 0.	-
instance-number *instance-number*	Specifies the number of consecutive instances to be collected from the start instance when the object type is set to **column**. The value is an integer that ranges from 0 to 65535. The value 0 indicates that the system stops collecting statistics at the end of the column. If the instance range specified by the *start-index* and *instances-number* parameters is beyond the actual instance range, the system collects statistics within the actual instance range. The default value is 0.	-

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **object** *oid* **class single** command creates a statistics object for the data item of a single instance. In this command, the *oid* parameter must contain the instance index. When the instance index is set to 0, the data item is a scalar quantity. When the instance index is set to a non-0 value, the data item is an instance in the column. If the object has been configured in the bulk file, the system displays an error message indicating that the OID already exists.

The **object** *oid* **class column start-index** *start-index* **instance-number** *instance-number* command creates a bulk statistics object to collect statistics about some or all types of instances in a column. You must specify the *start-index* and *instances-number* parameters to specify the start instance index and the number

of instances. If the instance range specified by the *start-index* and *instances-number* parameters is beyond the actual instance range, the system collects statistics within the actual instance range. If the object has been configured in the bulk file, the system displays an error message indicating that the OID already exists.

Precautions

The configuration of **object** or **undo object** takes effect in the next collection interval.

The OID specified in the command must exist in the MIB tree. If the specified OID exists in the bulk file, the system displays a message indicating that the OID has been configured. Delete this OID and then reconfigure it.

Example

Add a single statistics object to the bulk file **ifOutOctets**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file ifOutOctets
[HUAWEI-bulk-file-ifOutOctets] object 1.3.6.1.2.1.2.2.1.16.1 class single
```

Add a bulk statistics object to the bulk file **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] object 1.3.6.1.2.1.2.2.1.16 class column start-index 1 instance-number 10
```

16.1.28 reset snmp-agent statistics mib

Function

The **reset snmp-agent statistics mib** command clears statistics about the NMS's operations on MIB objects.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

reset snmp-agent statistics mib [**address** *ipv4-address* | **ipv6** *ipv6-address* | **vpn-instance** *vpn-instance-name* **address** *ipv4-address*]

Parameters

Parameter	Description	Value
address *ipv4-address*	Specifies an IPv4 address.	-

Parameter	Description	Value
ipv6 *ipv6-address*	Specifies an IPv6 address.	-
vpn-instance *vpn-instance-name*	Specifies a VPN instance name.	The value must be an existing VPN instance name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An NMS performs operations on MIB objects to manage devices. You can run the **display snmp-agent statistics mib** command to check the operation statistics.

If the NMS accesses a great amount of MIB node information and statistics do not need to be saved, run the **reset snmp-agent statistics mib** command to delete the statistics.

If no NMS is specified, the **reset snmp-agent statistics mib** command clears statistics about the operations performed by all NMSs (that is, IPv4+VPN, IPv6+VPN, IPv4, and IPv6 NMSs) on MIB objects.

Precautions

Operation statistics cannot be restored after they are cleared. Exercise caution when running the **reset snmp-agent statistics mib** command.

Example

Clear all statistics about the NMS's operations on MIB objects.

```
<HUAWEI> reset snmp-agent statistics mib
```

16.1.29 set snmp dynamic-control threshold

Function

The **set snmp dynamic-control threshold** command configures the CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks.

The **undo set snmp dynamic-control threshold** command restores the default setting.

By default, a device reduces resources for scheduling SNMP tasks when the CPU usage reaches 75%.

Format

set snmp dynamic-control threshold *threshold*

undo set snmp dynamic-control threshold *threshold*

Parameters

Parameter	Description	Value
threshold	Specifies the CPU usage threshold.	The value is an integer that ranges from 30 to 90, in percentage.

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks is 75%. That is, a device reduces resources for scheduling SNMP tasks when the CPU usage exceeds 75%. This reduces CPU usage of SNMP tasks. You can run the **set snmp dynamic-control threshold** command to change the CPU usage threshold based on your site scenario.

Example

Set the CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks to 60%.

```
<HUAWEI> system-view
[HUAWEI] set snmp dynamic-control threshold 60
Info: The CPU usage threshold that triggers a device to reduce resources for scheduling SNMP tasks is set to 60%. That is, when the system CPU usage exceeds 70%, the device reduces resources for scheduling SNMP tasks. Continue?[Y/N]:y
```

16.1.30 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

undo snmp-agent

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before configuring SNMP, you need to enable the SNMP agent function.

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

After the **snmp-agent** command is executed, both the IPv4 and IPv6 services are enabled for the SNMP agent. By default, the switch listens on the IP address 0.0.0.0, that is, all IP addresses. This default setting is a threat to data confidentiality. You are advised to run the **snmp-agent protocol source-interface** *interface-type interface-number* command to specify the source interface that receives and responds to SNMP requests from the NMS.

Example

Enable the SNMP agent function.

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

Disable the SNMP agent function.

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

16.1.31 snmp-agent acl

Function

The **snmp-agent acl** command configures an SNMP ACL.

The **undo snmp-agent acl** command deletes the configured SNMP ACL.

By default, no SNMP ACL is configured.

Format

snmp-agent acl { *acl-number* | *acl-name* }

snmp-agent acl-ipv4 { *acl-number* | *acl-name* } [**acl-ipv6** { *acl-number* | *acl-name* }]

snmp-agent acl-ipv6 { *acl-number* | *acl-name* }

undo snmp-agent acl

Parameters

Parameter	Description	Value
acl	Specifies an ACL that takes effect on both IPv4 and IPv6 networks.	-
acl-ipv4	Specifies an ACL that takes effect on only IPv4 network.	-
acl-ipv6	Specifies an ACL that takes effect on only IPv6 network.	-
acl-number	Specifies the number of an ACL.	The value is an integer ranging from 2000 to 3999.
acl-name	Specifies the name of a basic or an advanced Named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When using the NMS to manage devices, you can run the **snmp-agent acl** command to configure an SNMP ACL on the devices and restrict the NMS's access to the devices to enhance network security.

Precautions

- The SNMP ACLs take precedence over ACLs based on SNMP community names, SNMP groups, and SNMP users.
- To specify the same ACL on both IPv4 and IPv6 networks, you can only run the **snmp-agent acl** { *acl-number* | *acl-name* } command. For example, to allow the NMS that matches ACL 2000 to access the device using SNMP on

both IPv4 and IPv6 networks, run the **snmp-agent acl 2000** command instead of the **snmp-agent acl-ipv4 2000 acl-ipv6 2000** command.

- If this command is run more than once, the latest configuration overrides the previous one.

Example

Configure SNMP ACL 2000 to allow NM stations that match rules defined in ACL 2000 to access the device using SNMP.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-basic-2000] rule permit source 192.168.10.10 0
[HUAWEI-basic-2000] quit
[HUAWEI] snmp-agent acl 2000
```

16.1.32 snmp-agent blacklist ip-block disable

Function

The **snmp-agent blacklist ip-block disable** command disables the SNMP blacklist function.

The **undo snmp-agent blacklist ip-block disable** command enables the SNMP blacklist function.

By default, the SNMP blacklist function is enabled.

Format

snmp-agent blacklist ip-block disable

undo snmp-agent blacklist ip-block disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the SNMP blacklist function is enabled, if an SNMP user fails to connect to the device, the IP address used by the user is recorded in the SNMP blacklist on the device; that is, the IP address is locked. Within the locking period, the SNMP user cannot connect to the device.

If the connection fails to be established several times in succession, the device locks the IP address for 8 seconds on the first attempt, 16 seconds on the second attempt, and 32 seconds on the third attempt. Any subsequent failed attempts result in the IP address being locked for 5 minutes. When the locking period arrives, the IP address is automatically unlocked.

Precautions

After the SNMP blacklist function is disabled, the IP addresses of SNMP users who fail to connect to the device are not locked. The device is vulnerable to attacks and cracking by unauthorized users, affecting device security. Therefore, you are advised to enable the IP blacklist function.

After the SNMP blacklist function is disabled, locked IP addresses are unlocked immediately.

Example

Enable the SNMP blacklist function.

```
<HUAWEI> system-view
[HUAWEI] undo snmp-agent blacklist ip-block disable
```

16.1.33 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* | **cipher** *community-name* } [**mib-view** *view-name* | **acl** { *acl-number* | *acl-name* } | **alias** *alias-name*] *

snmp-agent community { **read** | **write** } [**cipher**] *community-name* [**mib-view** *view-name*] **acl-ipv4** { *acl-number* | *acl-name* } [**acl-ipv6** { *acl-number* | *acl-name* }] [**alias** *alias-name*]

snmp-agent community { **read** | **write** } [**cipher**] *community-name* [**mib-view** *view-name*] **acl-ipv6** { *acl-number* | *acl-name* } [**alias** *alias-name*]

undo snmp-agent community *community-name*

undo snmp-agent community { **read** | **write** } [**cipher**] *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 8 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
cipher *community-name*	Specifies the community name in plain text or in cipher text. The community name is displayed in cipher text in the configuration file.	The value is a string of 8 to 32, 44, 56, 80 or 88 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 8 to 31 characters, the string is processed as plain text by default and will be encrypted. • When the community name is a string of 32, 44, 56, 80 or 88 characters, the string is processed as cipher text by default, and the system will determine whether the string can be parsed.
mib-view *view-name*	Specifies a MIB view that the community name can access.	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	Specifies an ACL that takes effect on both IPv4 and IPv6 networks.	-
acl-ipv4	Specifies an ACL that takes effect on only IPv4 network.	-

Parameter	Description	Value
acl-ipv6	Specifies an ACL that takes effect on only IPv6 network.	-
acl-number	Specifies the number of an ACL.	The value is an integer ranging from 2000 to 3999.
acl-name	Specifies the name of a basic or an advanced Named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
alias *alias-name*	Specifies the alias name for a community. The alias names of communities are stored in plain text in the configuration file.	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

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **snmp-agent community** command is used on SNMPv1 and SNMPv2c networks. The community is a combination of the NMS and SNMP agent and is identified by a community name. The community name functions as a password for authentication during device communication in a community. Devices can communicate if the community name of the NMS and that of the SNMP agent are the same. The **snmp-agent community** command configures a community name on a device so that the NMS can communicate with the device. Parameters of the **snmp-agent community** command set the access permission, ACL, and accessible MIB views of a community name.

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**.
- The community name will be saved in encrypted format in the configuration file. To facilitate identification of community names, specify the **alias** *alias-name* parameter to set the alias names for the communities. The alias names are stored in plain text in the configuration file.

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.

Precautions

- The device checks the complexity of community names in simple text rather than in ciphertext. The device has the following requirements for community name complexity:
  - The minimum length of a community name is determined by the **set password min-length** command. By default, a password contains 8 characters.
  - The community name includes at least two kinds of characters: uppercase letters, lowercase letters, numbers, and special characters (excluding ?).

  If a community name fails the complexity check, the community name cannot be configured. To disable the complexity check for a community name, run the **snmp-agent community complexity-check disable** command, and then the length of community names in simple text ranges from 1 to 32. However, if a community name is simple and does not meet complexity requirements, it is prone to be attacked and cracked by unauthorized users, which affects device security. Therefore, enabling complexity check of community names is recommended.
- Only one type of permission can be configured for a community. If a community has both the read-only and read-write permission configured, the permission configured later takes effect.
- 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.
- The community name is saved in cipher text in the configuration file. To delete a community name, run the **undo snmp-agent community** *community name in plain text* or **undo snmp-agent community** *community name in plain text* command. To view a community name in cipher text, run the **display snmp-agent community** command.
- When a user with a level lower than the level configured using this command queries the password configured using the **display this** command, the password is displayed as asterisks (******).

- To specify the same ACL on both IPv4 and IPv6 networks, you can only run the **snmp-agent community** { **read** | **write** } { *community-name* | **cipher** *community-name* } **acl** { *acl-number* | *acl-name* } command.
- If the **snmp-agent community** command is run more than once to specify an ACL for the same SNMP community, the latest configuration overrides the previous one.
- If you forget the configured SNMP community name, run this command to configure a new one.

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
```

16.1.34 snmp-agent community complexity-check disable

Function

The **snmp-agent community complexity-check disable** command disables the complexity check of a community name.

The **undo snmp-agent community complexity-check disable** command enables the complexity check of a community name.

By default, the device enables the complexity check of a community name.

Format

snmp-agent community complexity-check disable

undo snmp-agent community complexity-check disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device checks the complexity of community names in simple text rather than in ciphertext. The device has the following requirements for community name complexity:

- The minimum length of a community name is determined by the **set password min-length** command. By default, a password contains 8 characters.
- The community name includes at least two kinds of characters: uppercase letters, lowercase letters, numbers, and special characters (excluding ?).

Precautions

To ensure the security of SNMP community names, enable the complexity check for community names. If a community name fails the complexity check, the community name cannot be configured. The complexity check can also be disabled for a community name. However, if a community name is simple and does not meet complexity requirements, it is prone to be attacked and cracked by unauthorized users, which affects device security.

Example

Disable the complexity check for community names.

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

16.1.35 snmp-agent community plaintext enable

Function

The **snmp-agent community plaintext enable** command enables SNMPv1 and SNMPv2c community names to be displayed in plaintext.

The **undo snmp-agent community plaintext enable** command enables SNMPv1 and SNMPv2c community names to be displayed in ciphertext.

By default, SNMPv1 and SNMPv2c community names are displayed in ciphertext.

Format

snmp-agent community plaintext enable

undo snmp-agent community plaintext enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage scenario

After you run the **snmp-agent community plaintext enable** command, the community name is displayed in plaintext after you run the **snmp-agent community** { **read** | **write** } *community-name* command to specify a plaintext community name.

Precautions

The existing community names are not affected after you run the **snmp-agent community plaintext enable** command. But the configured community names displayed in plaintext will be encrypted and displayed in ciphertext after you run the **undo snmp-agent community plaintext enable** command.

To ensure the security of community names, enable SNMPv1 and SNMPv2c community names to be displayed in ciphertext.

Example

Enable SNMPv1 and SNMPv2c community names to be displayed in ciphertext.

```
<HUAWEI> system-view
[HUAWEI] undo snmp-agent community plaintext enable
```

16.1.36 snmp-agent extend error-code enable

Function

The **snmp-agent extend error-code enable** command enables the device to send extended error codes to the NMS.

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

With the increasing number of features and scenarios supported by the system, the current types of SNMP standard error codes can hardly meet requirements in diversified scenarios. Therefore, the extended error code is introduced. The extended error code can define more scenarios for the NMS to correctly analyze the fault type of the current NE.

If both the NMS and managed device are Huawei products, 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 device to send extended error codes to the NMS.

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

16.1.37 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** | **privacy** | **noauthentication** } [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view*]* [**acl** { *acl-number* | *acl-name* }]

snmp-agent group v3 *group-name* { **authentication** | **privacy** | **noauthentication** } [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view*]* **acl-ipv4** { *acl-number* | *acl-name* } [**acl-ipv6** { *acl-number* | *acl-name* }]

snmp-agent group v3 *group-name* { **authentication** | **privacy** | **noauthentication** } [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view*]* **acl-ipv6** { *acl-number* | *acl-name* }

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

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.
authentication | **privacy** | **noauthentication**	Indicates the security level of the SNMP group. • **authentication**: authenticates SNMP messages without encryption. • **privacy**: authenticates and encrypts SNMP messages. • **noauthentication**: not authenticate or encrypt SNMP messages.	To ensure security, 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.

Parameter	Description	Value
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	Specifies an ACL that takes effect on both IPv4 and IPv6 networks.	-
acl-ipv4	Specifies an ACL that takes effect on only IPv4 network.	-
acl-ipv6	Specifies an ACL that takes effect on only IPv6 network.	-
acl-number	Specifies the number of an ACL.	The value is an integer ranging from 2000 to 3999.
acl-name	Specifies the name of a basic or an advanced Named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

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 the **noauthentication** parameter is set, 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.
- 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** command.

If non authentication and non encryption, or authentication and non encryption is configured for an SNMPv3 group, these modes bring security risks. To improve system security, delete the group and create a group with authentication and encryption.

To specify the same ACL on both IPv4 and IPv6 networks, you can only run the **snmp-agent group v3** *group-name* { **authentication** | **privacy** | **noauthentication** } [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view*]* **acl** { *acl-number* | *acl-name* } command.

If the **snmp-agent group** command is run more than once to specify an ACL for the same SNMP user group, the latest configuration overrides the previous one.

Example

Create an SNMPv3 group named **Johngroup** to authenticate and encrypt SNMP messages, and set the read-only view of the SNMPv3 group 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** to authenticate and encrypt SNMP messages, and set the write-only view of the SNMPv3 group 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
```

16.1.38 snmp-agent heartbeat enable

Function

The **snmp-agent heartbeat enable** command enables the device to send heartbeat packets to the NMS.

The **undo snmp-agent heartbeat enable** command disables the device from sending heartbeat packets to the NMS.

By default, the device does not send heartbeat packets to the NMS.

Format

snmp-agent heartbeat enable

undo snmp-agent heartbeat enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the NMS cannot initiatively obtain the status of the device, run the **snmp-agent heartbeat enable** command to enable the device to send heartbeat packets (corresponding trap: hwEntityHeartbeatTrap) to the NMS. The device then periodically sends heartbeat packets to the NMS to notify the NMS of its status.

Example

Enable the device to send heartbeat packets to the NMS.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent heartbeat enable
```

16.1.39 snmp-agent heartbeat interval

Function

The **snmp-agent heartbeat interval** command sets the interval at which the device sends heartbeat packets to the NMS.

The **undo snmp-agent heartbeat interval** command restores the interval at which the device sends heartbeat packets to the NMS to the default interval.

By default, the device sends heartbeat packets to the NMS at an interval of 60 seconds.

Format

snmp-agent heartbeat interval *interval*

undo snmp-agent heartbeat interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which the device sends heartbeat packets to the NMS.	The value is an integer that ranges from 60 to 86400, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the device to send heartbeat packets to the NMS, you can use the **snmp-agent heartbeat interval** command to set the interval at which heartbeat packets are sent. On a stable network, increase the interval to reduce the bandwidth consumed for periodic transmission of heartbeat packets.

Prerequisites

The device has been enabled to send heartbeat packets to the NMS using the **snmp-agent heartbeat enable** command.

Example

Configure the device to send heartbeat packets to the NMS at an interval of 180 seconds.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent heartbeat interval 180
```

16.1.40 snmp-agent inform

Function

The **snmp-agent inform** command sets global parameters of informs, including the timeout period for waiting for inform ACK messages, number of times to retransmit informs, and maximum number of informs to be confirmed in the inform buffer.

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

By default, the timeout waiting period for inform ACK messages is 15 seconds, the number of times to retransmit informs is 3, and the maximum number of informs in the inform buffer is 39.

Format

snmp-agent inform { **timeout** *seconds* | **resend-times** *times* | **pending** *number* } *

undo snmp-agent inform { **timeout** | **resend-times** | **pending** } *

Parameters

Parameter	Description	Value
timeout *seconds*	Specifies the timeout period for waiting for inform ACK messages from the NMS.	The value is an integer ranging from 1 to 1800, in seconds. The default value is 15 seconds.
resend-times *times*	Specifies the times to retransmit informs in the case that no inform ACK message is returned from the NMS.	The value is an integer ranging from 0 to 10. The default value is 3.
pending *number*	Specifies the maximum number of informs to be confirmed in the inform buffer.	The value is an integer ranging from 1 to 2048. The default value is 39.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After sending an inform, the SNMP agent waits for an inform ACK message from the NMS. You can run the **snmp-agent inform** command to set parameters **timeout**, **resend-times**, and **pending** of the inform.

These three parameters mutually affect each other. For example, if the timeout period for waiting for inform ACK messages prolongs or the times to retransmit informs increase, but the maximum number of informs to be confirmed is not changed, the number of informs to be confirmed is increased, causing the inform buffer to be quickly filled up.

Once the inform buffer is filled up, the earliest inform in the inform buffer is deleted each time a new inform enters the queue. The deleted informs are not retransmitted to the NMS. To avoid this problem, you can increase the maximum number of informs to be confirmed in the inform buffer.

You can configure the **snmp-agent inform** command to contain the parameter **timeout**, **resend-times**, or **pending** according to the network condition.

- When a large number of informs are dropped on the network, you can run the **snmp-agent inform pending** *number* command to increase the inform buffer.
- When the transmission speed on the network is low, you can increase the timeout period. Increasing the timeout period will increase the waiting time of informs in the inform buffer. You can also run the **snmp-agent inform** { **timeout** *seconds* | **pending** *number* } * command to increase the inform.

- When the transmission speed on the network is high, you can run the **snmp-agent inform timeout** *seconds* command to reduce the timeout period.
- When informs are transmitted on an unreliable network, you can increase the retransmission times. In this case, the informs in the inform buffer need to wait for a longer time to be confirmed. You can run the **snmp-agent inform** { **resend-times** *times* | **pending** *number* } * command to increase the inform buffer.

Prerequisites

Parameters for sending informs take effect only after the IP address of the target host for receiving informs is configured using the **snmp-agent target-host inform** command.

Precautions

You need to configure only parameters for sending informs using the **snmp-agent inform** command; you do not need to configure parameters for sending traps.

You must set the parameters **timeout**, **resend-times**, and **pending** according to the network condition. Otherwise, the SNMP working efficiency is greatly affected.

Example

Set the times to retransmit an inform to 5 and the maximum number of informs waiting to be confirmed in the inform buffer to 100.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent inform resend-times 5 pending 100
```

16.1.41 snmp-agent inform address

Function

The **snmp-agent inform address** command sets parameters for sending informs, including the timeout period for waiting for inform ACK messages from the NMS and times to retransmit an inform.

The **undo snmp-agent inform address** command restores the default setting for a particular inform host.

By default, the timeout waiting period for inform ACK messages is 15 seconds and the number of times to retransmit informs is 3.

Format

snmp-agent inform { **timeout** *seconds* | **resend-times** *times* } * **address udp-domain** *ip-address* [**vpn-instance** *vpn-instance-name*] **params securityname** { *security-name* | **cipher** *security-name* }

undo snmp-agent inform { **timeout** [*seconds*] | **resend-times** [*times*] } * **address udp-domain** *ip-address* [**vpn-instance** *vpn-instance-name*] **params securityname** { *security-name* | **cipher** *security-name* }

Parameters

Parameter	Description	Value
timeout *seconds*	Specifies the timeout period for waiting for inform ACK messages from the NMS.	The value is an integer ranging from 1 to 1800, in seconds. The default value is 15, which is equal to the global timeout period configured using the **snmp-agent inform** command.
resend-times *times*	Specifies the number of times that informs are retransmitted when no inform ACK message is returned from the NMS.	The value is an integer ranging from 0 to 10. The default value is 3, which is equal to the global retransmission times configured using the **snmp-agent inform** command.
address	Indicates the address of the target host for receiving SNMP traps. **NOTE** The IP address specified by **address** and the security name specified by **securityname** together identify a host.	The value is dotted decimal notation.
udp-domain *ip-address*	Specifies the IP address of a specified target host, with the transmission domain based on UDP.	The value is dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name. The parameter **vpn-instance** is optional. On a VPN network, you need to use the VPN instance specified by **vpn-instance**, IP address, and security name to identify a target host.
params	Indicates information about the target host that generates SNMP notifications.	-

Parameter	Description	Value
securityname *security-name*	Displays the name of the target host for receiving informs on the NMS. For SNMPv3, **securityname** must be configured as the user name. **securityname** configured on the host needs to be the same as that configured on the NMS, or the NMS cannot receive the trap messages sent from the host. For SNMPv2c, the NMS can receive trap messages from all hosts without having **securityname** configured. **securityname** is used to distinguish multiple hosts that generate trap messages.	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.
cipher *security-name*	Indicates the unencrypted or encrypted string of security name.	The value is a string of 1 to 32 case-sensitive characters or a string of 32, 48, 56, or 68 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. • When the community name is a string of 1 to 32 characters, the string is processed as plain text by default and will be encrypted. • When the community name is a string of 32, 48, 56, or 68 characters, the string is processed as cipher text by default, and the system will determine whether the string can be parsed.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use both the **snmp-agent inform address** command and the **snmp-agent inform** command to set parameters according to the network condition.

- When a large number of Inform messages are dropped on the network, you are recommended to run the **snmp-agent inform pending** *number* command to lengthen the trap queue and then the **snmp-agent inform address** command to specify the destination IP address and name of the target host.
- When the transmission speed on the network is low, you are recommended to increase the timeout period. Increasing the timeout period will surely increase the waiting time of informs in the trap queue for confirmation. In this case, you are also recommended to run the **snmp-agent inform** { **timeout** *seconds* | **pending** *number* }* command to lengthen the trap queue and then the **snmp-agent inform address** command to specify the destination address and the displayed user name.
- When the transmission speed on the network is high, you are recommended to run the **snmp-agent inform timeout** *seconds* **address udp-domain** *ip-address* **params securityname** *security-name* command to reduce the timeout period.
- When informs are transmitted on an unreliable network, you are recommended to increase the retransmission times. In this case, the informs in the trap queue need to wait for a longer time to be confirmed. This requires you to run the **snmp-agent inform** { **resend-times** *times* | **pending** *number* }* command to lengthen the trap queue and then the **snmp-agent inform address** command to specify the destination address and the displayed user name.

Prerequisites

Parameters for sending informs take effect only after the IP address of the target host for receiving informs is configured using the **snmp-agent target-host inform** command.

Precautions

- You need to configure only parameters for sending informs using the **snmp-agent inform address** command; you do not need to configure parameters for sending traps.
- You must set the parameters **timeout** and **resend-times** according to the network condition. Otherwise, the SNMP working efficiency is greatly affected.
- The priority set for the **timeout** and **resend-times** parameters using the **snmp-agent inform address** command is higher than that set for the **timeout** and **resend-times** parameters using the **snmp-agent inform** command. If both parameters in Inform mode and parameters using the **snmp-agent inform address** command are configured, parameters using the

snmp-agent inform address command take effect for a specified destination host.

- For SNMPv2c, when a user with a level lower than the level configured using this command queries the securityname configured using the **display this** command, the securityname is displayed as asterisks (******).

Example

Set the times to retransmit an inform to the target host (with the IP address of 10.1.1.1 and the security name of ABC) to 10.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent inform resend-times 10 address udp-domain 10.1.1.1 params securityname ABC
```

16.1.42 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*

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. It cannot be all 0s or all Fs.

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 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

- 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.
- If the local engine ID is set or changed, the existing SNMPv3 user with this engine ID is deleted.

Example

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

```
<HUAWEI> system-view
[HUAWEI] snmp-agent local-engineid 800007DB03360102101100
```

16.1.43 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 device has the MIB view ViewDefault with OID of 1.3.6.1.

For SNMPv1 and SNMPv2c, you can access the Viewdefault view by default. For SNMPv3, you must specify the MIB views that can be accessed by running the **snmp-agent group** command; if no new MIB view is created, you can specify the default MIB view ViewDefault in this command.

Format

snmp-agent mib-view { **excluded** | **included** } *view-name oid-tree*

undo snmp-agent mib-view *view-name* [*oid-tree*]

undo snmp-agent mib-view [**excluded** | **included**] *view-name* [*oid-tree*]

Parameters

Parameter	Description	Value
excluded	Indicates that the MIB view excludes the MIB subtree.	-
included	Indicates that the MIB view includes the MIB subtree.	-
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.
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.	It is a string of 1 to 255 case-sensitive characters without spaces. **NOTE** It must be a valid MIB subtree.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Most SNMP configuration commands contain the parameter *view-name*. The **snmp-agent mib-view** command is used to create or update a view. You cannot modify or delete the default ViewDefault MIB view.

In the **snmp-agent mib-view** command, the parameter *view-name* can be displayed as an OID or an object name.

- Displaying the parameter *view-name* as an OID: **snmp-agent mib-view included myview 1.3.6.1.2.1**.
- Displaying the parameter *view-name* as an object name: **snmp-agent mib-view excluded myview system.7**.

NOTE

To uniquely identify object identifiers in SNMP messages, SNMP uses a hierarchical naming structure to distinguish object identifiers from each other. This is a tree-like structure, with the nodes (such as {1.3.6.1.2.1}) representing object identifiers. The MIB is a collection of standard variables on monitored network devices.

You can select parameters based on the following rules:

- **excluded**: If a few MIB objects on the device or some objects in the current MIB view do not or no longer need to be managed by the NM station, **excluded** needs to be specified in the command to exclude these MIB objects.
- **included**: If a few MIB objects on the device or some objects in the current MIB view need to be managed by the NM station, **included** needs to be specified in the command to include these MIB objects.

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

When you run the **snmp-agent mib-view** command for multiple times to define the MIB view, the new configuration overwrites the original configuration if the values of *view-name* and *oid-tree* are the same; the new and original configurations both take effect if the values of *view-name* and *oid-tree* are different. The system can store a maximum of 256 MIB view configurations, among which there are four default views.

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 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.

Example

Create MIB view **mib2view** that includes all mib-2 objects and the subtree with the OID as 1.3.6.1.2.1.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent mib-view included mib2view 1.3.6.1.2.1
```

16.1.44 snmp-agent notification-log

Function

The **snmp-agent notification-log** command sets the aging time of trap logs and the maximum number of trap logs that can be saved in the trap log buffer.

The **undo snmp-agent notification-log** command restores the default configuration.

By default, the aging time of trap logs is 24 hours, and a maximum of 500 trap logs can be saved in the trap log buffer.

Format

snmp-agent notification-log { **global-ageout** *ageout* | **global-limit** *limit* } *

undo snmp-agent notification-log { **global-ageout** [*ageout*] | **global-limit** [*limit*] } *

Parameters

Parameter	Description	Value
global-ageout *ageout*	Specifies the aging time of trap logs.	The value can be 0 or an integer that ranges from 12 to 36, in hours. The default value is 24. The value 0 indicates that trap logs are never aged out.
global-limit *limit*	Specifies the maximum number of trap logs that can be saved in the trap log buffer.	The value is an integer that ranges from 1 to 5000.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a device sends the alarms propagated through Inform messages, the target host is required to respond with Inform ACK messages. In the following two situations, the alarms propagated through Inform messages are logged and the alarm logs are cached in the log buffer to help the target host synchronize the alarms generated in the event of host or link failures:

- No Inform ACK message is returned when the number of times to resend the Inform message in the alarm queue reaches the set threshold.
- Inform messages will be discarded because the number of logged Inform messages reaches the maximum that the alarm queue can support.

The maximum number of alarm logs in a log buffer is fixed (500 by default) to prevent a device from being burdened with excessive alarm logs. Alarm logs are aged periodically (24 hours by default) to ensure alarm logs remain up-to-date.

Precautions

- Only Inform logs are saved to the log buffer; trap logs are not saved to the log buffer.
- If notification logs in the log buffer do not need to be aged, you can set the aging time of these notification logs to 0.

- If the number of notification logs saved to the log buffer within the aging time exceeds the limit, new notification logs can still be saved but overwrites the earlier logs in the log buffer.
- The maximum number of alarm logs specified in the **snmp-agent notification-log** command cannot occupy more memory than the memory occupied by the log buffer. If the size of the log buffer is excessively large, more network resources are consumed. You are therefore recommended to set the size of the log buffer to a reasonable value.

Example

Set the aging time of trap logs to 36 hours.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent notification-log global-ageout 36
```

Set the maximum number of trap logs that can be saved in the trap log buffer to 1000.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent notification-log global-limit 1000
```

16.1.45 snmp-agent notification-log enable

Function

The **snmp-agent notification-log enable** command enables the notification logging function.

The **undo snmp-agent notification-log enable** command disables the notification logging function.

By default, the notification logging function is disabled.

Format

snmp-agent notification-log enable

undo snmp-agent notification-log enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the route from a network element to the NMS is unreachable because of a link failure between the network element and NMS, the network element does not send any SNMP notifications to the NMS. If the notification logging function is enabled, the network element records trap logs. When the link between the network element and NMS recovers, the NMS can obtain the trap logs recorded when the link was faulty.

After the notification logging function is enabled, the system records informs in trap logs in either of the following conditions:

- No ACK message is received after an inform in the notification queue is retransmitted the specified number of times.
- Earliest informs are discarded because the number of notifications in the notification queue exceeds the limit. The system records the discarded informs in trap logs.

Precautions

Only informs are recorded in trap logs, and traps are not recorded.

Example

Enable the notification logging function.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent notification-log enable
```

16.1.46 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 { **included** | **excluded** } *profile-name oid-tree*

undo snmp-agent notify-filter-profile [**included** | **excluded**] *profile-name*

Parameters

Parameter	Description	Value
included	Includes the specified MIB subtree.	-
excluded	Excludes the specified MIB subtree.	-

Parameter	Description	Value
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 255 case-sensitive characters without spaces. **NOTE** It must be a valid MIB subtree.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To filter trap messages sent to a target host, run the **snmp-agent notify-filter-profile** command to add the MIB objects to be filtered to a filter profile to limit the number of MIB objects that can send trap messages to the NMS. After the filter profile is configured using the **snmp-agent notify-filter-profile** command, only the trap messages generated by eligible MIB objects are sent to the NMS.

Precautions

- If no trap filter profile is configured, all traps are sent to the destination host.
- The **snmp-agent notify-filter-profile** command creates or updates a trap filter profile. The value of *oid-tree* can be an OID or a subtree name. An OID can contain asterisks (*) as wildcards. An asterisk (*) cannot be placed at the beginning or end of the OID string.
- In Include filtering mode of an alarm, OIDs of all bound variables in the alarm must be specified in this command. Otherwise, the filtering fails.
- In Exclude filtering mode of an alarm, only the OID of the alarm or that of any bound variable need to be specified in this command.

Example

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

```
<HUAWEI> system-view
[HUAWEI] snmp-agent notify-filter-profile included tmp 1.3.6.1.*.4
```


16.1.47 snmp-agent packet contextengineid-check enable

Function

The **snmp-agent packet contextengineid-check enable** command enables the device to check consistency between the contextEngineID on the NMS and the local engine ID.

The **undo snmp-agent packet contextengineid-check enable** command disables the device from checking consistency between the contextEngineID on the NMS and the local engine ID.

By default, the device does not check consistency between the contextEngineID on the NMS and the local engine ID.

Format

snmp-agent packet contextengineid-check enable

undo snmp-agent packet contextengineid-check enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the device does not check consistency between the contextEngineID on the NMS and the local engine ID, the NMS can connect to the device even if the contextEngineID is different from the local engine ID.

To improve system security, run the **snmp-agent packet contextengineid-check enable** command to enable the device to check consistency between the contextEngineID on the NMS and the local engine ID.

Configuration Impact

After this function is enabled, an NMS cannot connect to the device if the contextEngineID on the NMS is different from the local engine ID.

Precautions

This consistency check function applies only to SNMPv3.

Example

Enable the consistency check between the contextEngineID and local engine ID.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent packet contextengineid-check enable
```

16.1.48 snmp-agent packet max-size

Function

The **snmp-agent packet max-size** command sets the maximum size of an SNMP message.

The **undo snmp-agent packet max-size** command restores the default setting.

By default, the maximum size of an SNMP message is 12000 bytes.

Format

snmp-agent packet max-size *byte-count*

undo snmp-agent packet max-size

Parameters

Parameter	Description	Value
byte-count	Specifies the maximum size of an SNMP message that the SNMP agent can receive and send.	The value is an integer that ranges from 484 to 17940, in bytes. The default value is 12000.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You are recommended to run the **snmp-agent packet max-size** command to set the maximum size of an SNMP message that the SNMP agent receives or sends according to the network condition.

By increasing the maximum size of an SNMP message, you can prevent the NMS from obtaining the incomplete information about the device status.

By decreasing the maximum size of an SNMP message, you can prevent the NMS or device from discarding an SNMP message because its size exceeds the processing capability of the NMS or device.

Precautions

You need to increase the size of an SNMP message according to the network condition. Otherwise, the transmission efficiency of SNMP messages is affected.

Generally, the default value is recommended.

The maximum size set through the **snmp-agent packet max-size** command takes effect for the SNMP messages of all SNMP versions.

Example

Set the maximum size of an SNMP message that the SNMP agent can receive or send to 1042 bytes.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent packet max-size 1042
```

16.1.49 snmp-agent packet-priority

Function

The **snmp-agent packet-priority** command sets the priority of SNMP messages.

The **undo snmp-agent packet-priority** command restores the default priority of SNMP messages.

By default, the priority of SNMP messages is 6.

Format

snmp-agent packet-priority { **snmp** | **trap** } *priority-level*

undo snmp-agent packet-priority { **snmp** | **trap** }

Parameters

Parameter	Description	Value
snmp	Sets the priority of common SNMP messages (excluding trap messages), including: • Get-Response packets • Set-Response packets	-
trap	Sets the priority of SNMP trap messages, including: • Trap packets • Inform packets	-

Parameter	Description	Value
priority-level	Specifies the priority of SNMP messages.	The value is an integer that ranges from 0 to 7. The default value is 6. The value 0 indicates the lowest priority, and the value 7 indicates the highest priority.

Views

System view

Default Level

3: Management level

Usage Guidelines

SNMP messages may be lost if the number of SNMP messages on a network exceeds the processing capability of the NMS. Run the **snmp-agent packet-priority** command to set the transmission priority of SNMP messages to ensure that the NMS can process important messages first. This command can be used in the following situations:

- To prevent traps from being discarded, increase the priority of SNMP trap messages so that traps can be successfully sent to the NMS.
- To improve reliability of MIB operations performed on the device by the NMS, increase the priority of common SNMP messages, excluding SNMP trap messages.
- When the network is severely congested and traps are generated frequently, reduce the priority of all SNMP messages, including SNMP trap messages.

Example

Set the priority of common SNMP messages to 5.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent packet-priority snmp 5
```

16.1.50 snmp-agent protocol get-bulk timeout

Function

The **snmp-agent protocol get-bulk timeout** command configures a get-bulk operation timeout period.

The **undo snmp-agent protocol get-bulk timeout** command restores the default get-bulk operation timeout period.

The default get-bulk operation timeout period is 2 seconds.

Format

snmp-agent protocol get-bulk timeout *time*

undo snmp-agent protocol get-bulk timeout

Parameters

Parameter	Description	Value
time	Specifies a get-bulk operation timeout period.	The value is an integer ranging from 0 to 600, in seconds. **NOTE** The value 0 indicates that a get-bulk operation never expires.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A get-bulk operation allows an NMS to query information about multiple managed devices at a time, equaling multiple get-next operations.

If an NMS requests many data through a get-bulk operation, a long time is required to obtain the data. You can run the **snmp-agent protocol get-bulk timeout** command to change the get-bulk operation timeout period.

Precautions

You are not advised to change the get-bulk operation timeout period. The default get-bulk operation timeout period is recommended. To reconfigure a get-bulk operation timeout period, you must ensure that the configured period is less than an NMS's timeout period.

Example

Set the get-bulk operation timeout period to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent protocol get-bulk timeout 10
```


16.1.51 snmp-agent protocol ipv6 source-ip

Function

The **snmp-agent protocol ipv6 source-ip** command configures an IPv6 address for receiving and responding to NMS requests.

The **undo snmp-agent protocol ipv6 source-ip** command restores the default configuration.

By default, no IPv6 address can be used to receive or respond to NMS requests.

Format

snmp-agent protocol ipv6 source-ip *ipv6-address* [**vpn-instance** *vpn-instance-name*]

undo snmp-agent protocol ipv6 source-ip

Parameters

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address.	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.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, no IPv6 address can be used to receive or respond to NMS requests. When a device needs to establish a connection with the NMS, you can run the **snmp-agent protocol ipv6 source-ip** command to specify an IPv6 address for the device to receive and respond to NMS requests.

Precautions

- After the **snmp-agent protocol ipv6 source-ip** command is run, the NMS can communicate with the device only through the specified IPv6 address.

Therefore, ensure that there are reachable routes between the NMS and the specified IPv6 address.

- If you run this command multiple times, only the latest configuration takes effect.

Example

Configure 1::1 as a IPv6 address for receiving and responding to NM station requests.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent protocol ipv6 source-ip 1::1
```

16.1.52 snmp-agent protocol server disable

Function

The **snmp-agent protocol server disable** command disables the SNMP IPv4 or IPv6 listening port.

The **undo snmp-agent protocol server disable** command enables the SNMP IPv4 or IPv6 listening port.

By default, the SNMP IPv4 or IPv6 listening port is disabled.

Format

snmp-agent protocol server [**ipv4** | **ipv6**] **disable**

undo snmp-agent protocol server [**ipv4** | **ipv6**] **disable**

Parameters

Parameter	Description	Value
ipv4	Disables the SNMP IPv4 listening port.	-
ipv6	Disables the SNMP IPv6 listening port.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable alarm sending to the NMS without performing the Get/Set operation, SNMP port listening is not required. To disable the SNMP IPv4 or IPv6 listening port, run the **snmp-agent protocol server disable** command.

This command helps separately manage and control SNMP IPv4 and IPv6 listening ports.

If **ipv4** or **ipv6** is not selected, both SNMP IPv4 and IPv6 listening ports are disabled.

Precautions

After you disable the SNMP IPv4 or IPv6 listening port using the **snmp-agent protocol server disable** command, SNMP no longer processes SNMP packets. Exercise caution when you disable the SNMP IPv4 or IPv6 listening port.

Example

Disable the SNMP IPv4 listening port.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent protocol server ipv4 disable
```

16.1.53 snmp-agent protocol source-interface

Function

The **snmp-agent protocol source-interface** command configures an interface for receiving and responding to NMS requests.

The **undo snmp-agent protocol source-interface** command restores the default configuration.

By default, no interface can receive or respond to NMS requests.

Format

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

undo snmp-agent protocol source-interface

Parameters

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

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, no interface can receive or respond to NMS requests. When a device needs to establish a connection with the NMS, you can run the **snmp-agent protocol source-interface** command to specify an interface on the device to receive and respond to NMS requests.

Prerequisites

The interface to be configured as the interface must have been created, and a valid IP address must have been assigned to this interface. If the interface to be configured as the interface is not created or a valid IP address is not assigned to the interface, the **snmp-agent protocol source-interface** command will not take effect. If a valid IP address is assigned to the interface, the **snmp-agent protocol source-interface** command will take effect automatically.

Precautions

- If the interface on which the **snmp-agent protocol source-interface** command is configured is deleted, or an address is changed or deleted on the interface, SNMP configurations will not be affected.
- After SNMP is bound to the interface, SNMP listens only this interface, through which the NMS communicates with the device. If the interface or its IP address is deleted, SNMP will stop receiving IP packets, and therefore communication between the NMS and devices will interrupt. After the interface's IP address is changed, the NMS can communicate with devices only through the new IP address.
- If you run this command multiple times, only the latest configuration takes effect.

Example

Configure loopback 1 for receiving and responding to NMS requests.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent protocol source-interface Loopback 1
```

16.1.54 snmp-agent protocol source-status

Function

The **snmp-agent protocol source-status** command enables all interfaces or IPv6 addresses to receive and respond to NMS requests.

The **undo snmp-agent protocol source-status** command restores the default configuration.

By default, no interface or IPv6 address can be used to receive or respond to NMS requests.

Format

snmp-agent protocol source-status [**ipv6**] **all-interface**

undo snmp-agent protocol source-status [**ipv6**] **all-interface**

Parameters

Parameter	Description	Value
ipv6	Enables all IPv6 addresses to receive and respond to NMS requests.	-
all-interface	Enables all interfaces to receive and respond to NMS requests.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

For security purposes, no interface or IPv6 address can be used to receive or respond to NMS requests by default. When a device needs to establish a connection with the NMS, you can run any one of the following commands to allow the device to receive and respond to NMS requests:

- **snmp-agent protocol source-status**: Enables all interfaces or IPv6 addresses to receive and respond to NMS requests.
- **snmp-agent protocol source-interface**: Enables a specified interface to receive and respond to NMS requests.
- **snmp-agent protocol ipv6 source-ip**: Enables a specified IPv6 address to receive and respond to NMS requests.

Precautions

- Assume that on a switch running a version earlier than V200R020C00, the **snmp-agent** command is configured to enable the SNMP agent function, and the **snmp-agent protocol source-interface** and **snmp-agent protocol ipv6 source-ip** commands are not configured. After the switch is upgraded to V200R020C00 or a later version, the **snmp-agent protocol source-status all-interface** and **snmp-agent protocol source-status ipv6 all-interface** commands are automatically added to the configuration file.
- When the **snmp-agent protocol source-status** command is configured, all interfaces or IPv6 addresses can receive and respond to NMS requests, increasing system security risks. Therefore, this configuration is not recommended. You are advised to specify an interface or IPv6 address to receive and respond to NMS requests.

Example

Enable all interfaces to receive and respond to NMS requests.


```
<HUAWEI> system-view
[HUAWEI] snmp-agent protocol source-status all-interface
```

16.1.55 snmp-agent protocol server message queue

Function

The **snmp-agent protocol server message queue** command configures the size of a packet queue that can be received by an SNMP agent.

The **undo snmp-agent protocol server message queue** command restores the default size.

By default, the packet queue that can be received by an SNMP agent contains 30 packets.

Format

snmp-agent protocol server message queue *message-queue*

undo snmp-agent protocol server message queue

Parameters

Parameter	Description	Value
message-queue	Specifies the size of a packet queue.	The value is an integer ranging from 10 to 100.

Views

System view

Default Level

3: Management level

Usage Guidelines

If some packets are discarded when the number of packets in the packet queue that can be received by an SNMP agent has reached the upper limit, run the **snmp-agent protocol server message queue** command to adjust the queue size.

Example

Configure the packet queue that can be received by an SNMP agent to contain 50 packets at most.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent protocol server message queue 50
```


16.1.56 snmp-agent statistics mib disable

Function

The **snmp-agent statistics mib disable** command disables the statistics function about the NMS's operations on MIB objects.

The **undo snmp-agent statistics mib disable** command restores the default statistics status.

By default, the statistics function about the NMS's operations on MIB objects is enabled.

NOTE

Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

snmp-agent statistics mib disable

undo snmp-agent statistics mib disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An NMS performs operations on MIB objects to manage devices. Currently, SNMP supports the statistics function about these operations.

By default, the statistics function is enabled. To disable this function due to some reasons, for example, high CPU usage caused by collecting statistics about the NMS accessing MIB objects, run the **snmp-agent statistics mib disable** command.

Follow-up Procedure

Run the **display snmp-agent statistics mib** command to check statistics about the NMS's operations on MIB objects.

If the NMS accesses a great amount of MIB node information and statistics do not need to be saved, run the **reset snmp-agent statistics mib** command to delete the statistics.

Precautions

After you run the **snmp-agent statistics mib disable** command, the statistics function is disabled, but statistics that have been collected are not deleted.

Example

Disable the statistics function about the NMS's operations on MIB objects.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent statistics mib disable
```

16.1.57 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 Beijing, Huawei Technologies Co., Ltd.", the system location is "Beijing 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.

Parameter	Description	Value
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. **NOTE** This parameter can be repeatedly configured. If a device runs multiple SNMP versions, the NMS can use any one of them to manage the device.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

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
- Supporting Inform messages

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 v3.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent sys-info version v3
```

16.1.58 snmp-agent target-host inform

Function

The **snmp-agent target-host inform** command sets the target host for receiving Inform messages.

The **undo snmp-agent target-host** command cancels the target host set to receive Inform messages.

By default, the target host for receiving Inform messages is not set.

Format

snmp-agent target-host inform address udp-domain *ip-address* [**udp-port** *port-number* | **source** *interface-type interface-number* | [**vpn-instance** *vpn-instance-name* | **public-net**]] * **params securityname** { *security-name* | **cipher** *security-name* } **v2c** [**notify-filter-profile** *profile-name* | **ext-vb**] *

snmp-agent target-host inform address udp-domain *ip-address* [**udp-port** *port-number* | **source** *interface-type interface-number* | [**vpn-instance** *vpn-instance-name* | **public-net**]] * **params securityname** *security-name* **v3** [**authentication** | **privacy**] [**notify-filter-profile** *profile-name* | **ext-vb**] *

undo snmp-agent target-host *ip-address* **securityname** { *security-name* | **cipher** *security-name* } [**vpn-instance** *vpn-instance-name*]

undo snmp-agent target-host inform address udp-domain *ip-address* [**udp-port** *port-number* | **source** *interface-type interface-number* | [**vpn-instance** *vpn-instance-name* | **public-net**]] * **params securityname** { *security-name* | **cipher** *security-name* }

Parameters

Parameter	Description	Value
address	Specifies the IP address of a specified target host.	-
udp-domain *ip-address*	Specifies the IP address of a specified target host, with the transmission domain being based on UDP.	It is dotted decimal notation.
udp-port *port-number*	Specifies the UDP port of the specified target host for receiving Inform messages.	The value is an integer ranging from 0 to 65535. The default value is 162.
source *interface-type interface-number*	Specifies the source interface of the device for sending Inform messages.	-
vpn-instance *vpn-instance-name*	Specifies VPN instance to which the target host belongs.	The value must be an existing VPN instance name.
public-net	Indicates the target host is on the public network.	-
params	Indicates information about the target host that generates SNMP notifications.	-

Parameter	Description	Value
securityname *security-name*	Specifies the user security name displayed on the NMS. For SNMPv3, **securityname** must be configured as the user name. **securityname** configured on the host needs to be the same as that configured on the NMS, or the NMS cannot receive the trap messages sent from the host. Ensure that the *security-name* value is the same as the created user name; otherwise, the NMS cannot access the device. For SNMPv1 and SNMPv2c, the NMS can receive trap messages from all hosts without having **securityname** configured. **securityname** is used to distinguish multiple hosts that generate trap messages.	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.

Parameter	Description	Value
cipher *security-name*	Indicates the unencrypted or encrypted string of security name.	The value is a string of 1 to 32 case-sensitive characters or a string of 32, 48, 56, or 68 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. ● When the community name is a string of 1 to 32 characters, the string is processed as plain text by default and will be encrypted. ● When the community name is a string of 32 48, 56, or 68 characters, the string is processed as cipher text by default, and the system will determine whether the string can be parsed.
v2c	Indicates the SNMP version is SNMPv2c.	-
v3	Indicates the SNMP version is SNMPv3.	-
authentication | **privacy**	Specifies the security mode. ● **authentication**: authenticates SNMP messages without encryption. ● **privacy**: authenticates and encrypts SNMP messages. This parameter takes effect only in SNMPv3.	-

Parameter	Description	Value
notify-filter-profile *profile-name*	Specifies the filtering view name.	The filtering view must exist.
ext-vb	Indicates that traps sent to a target host carry extended bound variables. If a Huawei data communication device extends the trap objects defined in the public MIB, you can configure this parameter to determine whether traps sent to the NMS carry extended bound variables. • If this parameter is not configured, the traps sent from the Huawei data communication device do not carry extended bound variables. If you are using a third-party NMS tool, you are not advised to configure this parameter, which ensures that the NMS tool can receive alarms sent from the Huawei device. By default, a trap sent from a Huawei data communication device does not carry extended bound variables. • If this parameter is configured, the traps sent from the Huawei data communication device carry extended bound variables. If you are using a Huawei NMS tool, you are advised to configure this parameter, which allows you to view more information carried in a trap.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After sending an Inform message, the device waits for an Inform ACK message from the NMS and will retransmit the same Inform message only when no Inform ACK message is received from the NMS within the specified period. If the SNMP agent does not receive the inform ACK message from the NMS during the retransmission period, the SNMP agent deletes this inform message from the trap queue. This ensures that the NMS can receive the SNMP Inform messages to the maximum extent.

If there are multiple target hosts, you need to run the **snmp-agent target-host inform** command on each target host. If the **snmp-agent target-host inform** command is executed for multiple times on the target host, only the last successful operation takes effect.

The rules for selecting the target host are as follows:

- If the **public-net** parameter is specified, the system accesses the target host on the public network.
- If the **vpn-instance** *vpn-instance-name* parameter is specified, the system accesses the target host in the specified VPN instance.
- If both the **public-net** and **vpn-instance** *vpn-instance-name* parameters are not specified:
  a. If the **source** *interface-type interface-number* parameter is specified and a VPN instance is bound to the specified interface, the system accesses the target host in the VPN instance. If no VPN instance is bound to the specified interface, the system accesses the target host on the public network.
  b. If the **snmp-agent trap source** command is run to configure a source interface for sending trap packets and a VPN instance is bound to the interface, the system accesses the target host in the VPN instance. If no VPN instance is bound to the interface, the system accesses the target host on the public network.
  c. If the **set net-manager vpn-instance** command is run to configure a network management VPN instance, the system accesses the target host in this VPN instance.
  d. If none of the preceding conditions is met, the system accesses the target host on the public network.

Configuration Impact

The transmission of Inform messages, however, consumes more resources than that of traps.

Precautions

The **snmp-agent notify-filter-profile** command is used to create or update the trap filtering information. The NMS filters trap messages according to the profile and sends only the eligible trap messages to the target host. If **notify-filter-profile** is not configured, all trap messages are sent to the target host.

Ensure that the security level of a trap host is not higher than that of the user specified by **securityname** and not lower than that of the user group. Otherwise,

the trap host cannot send trap messages properly. The user security level can be (in descending order):

- Level 1: privacy (authentication and encryption)
- Level 2: authentication (without encryption)
- Level 3: noauthentication (no authentication or encryption)

When SNMPv3 is used to send Inform messages, run the **snmp-agent remote-engineid usm-user v3** command to configure a remote SNMPv3 user whose remote engine ID must be the same as the engine ID of the destination host.

The **securityname** configuration of an SNMPv2c alarm host is displayed in ciphertext, whereas the **securityname** configuration of an SNMPv3 alarm host is displayed in simple text. For SNMPv2c, when a user with a level lower than the level configured using this command queries the securityname configured using the **display this** command, the securityname is displayed as asterisks (******).

Example

Configure alarms to be sent in inform mode, set the security name of the host to 123 and protocol version to SNMPv3, and send alarms to the NMS host with the IP address of 192.168.10.1.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable
[HUAWEI] snmp-agent target-host inform address udp-domain 192.168.10.1 params securityname 123 v3
```

16.1.59 snmp-agent target-host trap

Function

The **snmp-agent target-host trap** command configures the target host for receiving SNMP traps.

The **undo snmp-agent target-host** command deletes the target host configuration for receiving SNMP traps.

By default, the target host is not set.

Format

snmp-agent target-host trap address udp-domain *ip-address* [**udp-port** *port-number* | **source** *interface-type interface-number* | [**public-net** | **vpn-instance** *vpn-instance-name*]] * **params securityname** *security-name* [[**v1** | **v2c** | **v3** [**authentication** | **privacy**]] | **private-netmanager** | **notify-filter-profile** *profile-name* | **ext-vb**] *

snmp-agent target-host trap address udp-domain *ip-address* [**udp-port** *port-number* | **source** *interface-type interface-number* | [**public-net** | **vpn-instance** *vpn-instance-name*]] * **params securityname cipher** *security-name* [[**v1** | **v2c**] | **private-netmanager** | **notify-filter-profile** *profile-name* | **ext-vb**] *

undo snmp-agent target-host *ip-address* **securityname** { *security-name* | **cipher** *security-name* } [**vpn-instance** *vpn-instance-name*]

undo snmp-agent target-host trap address udp-domain *ip-address* [**udp-port** *port-number* | **source** *interface-type interface-number* | [**public-net** | **vpn-instance** *vpn-instance-name*]] * **params securityname** { *security-name* | **cipher** *security-name* }

Parameters

Parameter	Description	Value
address	Specifies the IP address of a specified target host.	-
udp-domain *ip-address*	Specifies the IP address of a specified target host, with the transmission domain being based on UDP.	-
udp-port *port-number*	Specifies the UDP port of the specified target host for receiving Trap messages.	The value is an integer ranging from 0 to 65535. The default value is 162.
source *interface-type interface-number*	Specifies the source interface of the device for sending Trap messages.	-
public-net	Specifies VPN instance to which the target host belongs.	-
vpn-instance *vpn-instance-name*	Indicates the target host is on the public network.	The value must be an existing VPN instance name.

Parameter	Description	Value
params securityname *security-name*	Specifies the user security name displayed on the NMS. For SNMPv3, **securityname** must be configured as the user name. **securityname** configured on the host needs to be the same as that configured on the NMS, or the NMS cannot receive the trap messages sent from the host. Ensure that the *security-name* value is the same as the created user name; otherwise, the NMS cannot access the device. For SNMPv1 and SNMPv2c, the NMS can receive trap messages from all hosts without having **securityname** configured. **securityname** is used to distinguish multiple hosts that generate trap messages.	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.

Parameter	Description	Value
cipher *security-name*	Indicates the unencrypted or encrypted string of security name.	The value is a string of 1 to 32 case-sensitive characters or a string of 32, 48, 56, or 68 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. ● When the community name is a string of 1 to 32 characters, the string is processed as plain text by default and will be encrypted. ● When the community name is a string of 32 48, 56, or 68 characters, the string is processed as cipher text by default, and the system will determine whether the string can be parsed.
v1 | **v2c** | **v3**	Indicates the SNMP version. ● **v1**: SNMPv1. ● **v2c**: SNMPv2c. ● **v3**: SNMPv3. If this parameter is not specified, the default version is SNMPv1.	-

Parameter	Description	Value
authentication | **privacy**	Specifies the security mode. • **authentication**: authenticates packets without encryption. • **privacy**: authenticates and encrypts SNMP messages. This parameter takes effect only in SNMPv3.	-
private-netmanager	Indicates the Huawei NMS as the target host receiving a trap. When a Huawei NMS is deployed and this parameter is configured, a trap sent to the NMS contains more information, such as the trap type, sequence of the trap, and sending time.	-
notify-filter-profile *profile-name*	Specifies the filtering view name. If the trap filtering is not configured using the parameter **notify-filter-profile**, all traps will be sent to the destination host.	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.

Parameter	Description	Value
ext-vb	Indicates that traps sent to a target host carry extended bound variables. If a Huawei data communication device extends the trap objects defined in the public MIB, you can configure this parameter to determine whether traps sent to the NMS carry extended bound variables. • If this parameter is not configured, the traps sent from the Huawei data communication device do not carry extended bound variables. If you are using a third-party NMS tool, you are not advised to configure this parameter, which ensures that the NMS tool can receive alarms sent from the Huawei device. By default, a trap sent from a Huawei data communication device does not carry extended bound variables. • If this parameter is configured, the traps sent from the Huawei data communication device carry extended bound variables. If you are using a Huawei NMS tool, you are advised to configure this parameter, which allows you to view more information carried in a trap.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SNMP notifications can be classified into traps and inform messages. Trap messages are less reliable than inform messages because the NMS does not send

any acknowledgment when it receives a trap. In this case, the sender cannot verify whether the trap has been received. Informs are configured with an acknowledgment mechanism and therefore are reliable.

To configure multiple target hosts, you must run the **snmp-agent target-host trap** command on each target host. If you run the **snmp-agent target-host trap** command for multiple times on a host, only the latest configuration takes effect. For example, if you configure the trap function for a host that has been configured with trap, the second configuration takes effect.

The rules for selecting the target host are as follows:

- If the **public-net** parameter is specified, the system accesses the target host on the public network.
- If the **vpn-instance** *vpn-instance-name* parameter is specified, the system accesses the target host in the specified VPN instance.
- If both the **public-net** and **vpn-instance** *vpn-instance-name* parameters are not specified:
  a. If the **source** *interface-type interface-number* parameter is specified and a VPN instance is bound to the specified interface, the system accesses the target host in the VPN instance. If no VPN instance is bound to the specified interface, the system accesses the target host on the public network.
  b. If the **snmp-agent trap source** command is run to configure a source interface for sending trap packets and a VPN instance is bound to the interface, the system accesses the target host in the VPN instance. If no VPN instance is bound to the interface, the system accesses the target host on the public network.
  c. If the **set net-manager vpn-instance** command is run to configure a network management VPN instance, the system accesses the target host in this VPN instance.
  d. If none of the preceding conditions is met, the system accesses the target host on the public network.

Configuration Impact

No matter whether a trap sent from the SNMP agent reaches the NMS, the SNMP agent deletes the trap to reduce the resource consumption.

Precautions

Ensure that the security level of a trap host is not higher than that of the user specified by **securityname** and not lower than that of the user group. Otherwise, the trap host cannot send trap messages properly. The user security level can be (in descending order):

- Level 1: privacy (authentication and encryption)
- Level 2: authentication (without encryption)
- Level 3: noauthentication (no authentication or encryption)

If the SNMP trap function has been enabled, to ensure that SNMPv3-running devices normally send trap messages, **notify-view** *notify-view* must be configured in the **snmp-agent group** command for the user group to which **securityname** belongs to allow the devices to have the right to send trap messages.

For SNMPv1 and SNMPv2c, when a user with a level lower than the level configured using this command queries the securityname configured using the **display this** command, the securityname is displayed as asterisks (******).

Example

Allow the SNMP agent to send SNMP traps to the target host with the IP address of 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable
[HUAWEI] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname comaccess
```

Allow the SNMP agent to send SNMP traps to the Huawei NMS with the IP address of 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable
[HUAWEI] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname comaccess
private-netmanager
```

16.1.60 snmp-agent target-host trap ipv6

Function

The **snmp-agent target-host trap ipv6** command configures a target host to receive SNMP trap messages.

The **undo snmp-agent target-host ipv6** command deletes the configuration of a target host to receive SNMP trap messages.

By default, the target host that receives SNMP trap messages is not set.

Format

snmp-agent target-host trap ipv6 address udp-domain *ipv6-address* [**udp-port** *port-number* | **vpn-instance** *vpn-instance-name*] * **params securityname** *security-name* [[**v1** | **v2c** | **v3** [**authentication** | **privacy**]] | **private-netmanager** | **notify-filter-profile** *profile-name* | **ext-vb**] *

snmp-agent target-host trap ipv6 address udp-domain *ipv6-address* [**udp-port** *port-number* | **vpn-instance** *vpn-instance-name*] * **params securityname cipher** *security-name* [[**v1** | **v2c**] | **private-netmanager** | **notify-filter-profile** *profile-name* | **ext-vb**] *

undo snmp-agent target-host ipv6 *ipv6-address* **securityname** { *security-name* | **cipher** *security-name* } [**vpn-instance** *vpn-instance-name*]

undo snmp-agent target-host trap ipv6 address udp-domain *ipv6-address* [**udp-port** *port-number* | **vpn-instance** *vpn-instance-name*] * **params securityname** { *security-name* | **cipher** *security-name* }

Parameters

Parameter	Description	Value
ipv6 address	Sets the IPv6 address of the target host used to receive SNMP trap messages.	-
udp-domain	Indicates that trap messages are sent to the target host through the User Datagram Protocol (UDP).	-
ipv6-address	Specifies the IPv6 address of the target host.	-
udp-port *port-number*	Specifies the port number used to receive trap messages.	The value is an integer that ranges from 0 to 65535. The default value is 162.
vpn-instance *vpn-instance-name*	Specifies a VPN instance name. If the **vpn-instance** *vpn-instance-name* parameter is not specified, the system accesses the target host on the public network. The device cannot send traps to a target host on the VPN interface specified by the **set net-manager vpn-instance** command.	The **vpn-instance** parameter is optional. If **vpn-instance** is configured, the VPN instance specified by **vpn-instance** *vpn-instance-name*, IP address, and security name specified by **securityname** *security-string* form a 3-tuple to identify a host on a VPN.

Parameter	Description	Value
params securityname *security-name*	Specifies the SNMP security name that is displayed as the user name on the NMS. For SNMPv3, **securityname** must be configured as the user name. **securityname** configured on the host needs to be the same as that configured on the NMS, or the NMS cannot receive the trap messages sent from the host. For SNMPv1 and SNMPv2c, the NMS can receive trap messages from all hosts without having **securityname** configured. **securityname** is used to distinguish multiple hosts that generate trap messages.	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.
cipher *security-name*	Indicates the unencrypted or encrypted string of security name.	The value is a string of 1 to 32 case-sensitive characters or a string of 32, 48, 56, or 68 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. • When the community name is a string of 1 to 32 characters, the string is processed as plain text by default and will be encrypted. • When the community name is a string of 32 48, 56, or 68 characters, the string is processed as cipher text by default, and the system will determine whether the string can be parsed.

Parameter	Description	Value
v1 | **v2c** | **v3**	Specifies the SNMP version. ● **v1**: indicates SNMPv1. ● **v2c**: indicates SNMPv2c. ● **v3**: indicates SNMPv3. If no SNMP version is specified, SNMPv1 is used by default.	-
authentication | **privacy**	Specifies the security mode for SNMP trap messages. ● **authentication**: indicates that the SNMP trap messages are authenticated but not encrypted. ● **privacy**: indicates that SNMP trap messages are authenticated and encrypted.	-
private-netmanager	Indicates that the target host is a Huawei NMS. Specify this parameter when a Huawei NMS is used. This parameter enables trap messages sent to the NMS to contain more information, including types, sequence numbers, and transmission time of trap messages.	-
notify-filter-profile *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.

Parameter	Description	Value
ext-vb	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 **ext-vb** to determine whether the trap messages sent to the NMS carry extended bound variables. • If **ext-vb** is not specified, trap messages sent from the device do not carry extended bound variables. When a third-party NMS is used, you are advised not to specify the **ext-vb** parameter so that the third-party NMS can receive trap messages from Huawei data communication devices. By default, trap messages sent from a Huawei data communication device do not carry extended bound variables. • If **ext-vb** is specified, trap messages sent from the device carry extended bound variables. This parameter is recommended when a Huawei NMS is used so that more information can be transmitted in trap messages.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command is used to configure an IPv6 NMS host so that traps can be sent to the host using the IPv6 protocol.

Precautions

Ensure that the security level of a trap host is not higher than that of the user specified by **securityname** and not lower than that of the user group. Otherwise, the trap host cannot send trap messages properly. The user security level can be (in descending order):

- Level 1: privacy (authentication and encryption)
- Level 2: authentication (without encryption)
- Level 3: noauthentication (no authentication or encryption)

For SNMPv1 and SNMPv2c, when a user with a level lower than the level configured using this command queries the securityname configured using the **display this** command, the securityname is displayed as asterisks (******).

Example

Configure an IPv6 NMS host that uses SNMP v3. Set the security name to Test and configure traps to be authenticated and encrypted.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable
Warning: All switches of SNMP trap/notification will be open. Continue? [Y/N]:y
[HUAWEI] snmp-agent target-host trap ipv6 address udp-domain FC00::1 params securityname Test v3 privacy
```

16.1.61 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

2: Configuration 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.

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
```

16.1.62 snmp-agent trap enable

Function

The **snmp-agent trap enable** command enables the switch 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

2: Configuration level

Usage Guidelines

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

- To disable the trap function for all modules, run the **snmp-agent trap disable** command.
- To enable the trap function for a specified module, run the **snmp-agent trap enable feature-name** *feature-name* command.
- To disable the trap function for a specified module, run the **undo snmp-agent trap enable feature-name** *feature-name* command.
- To enable a specified trap for a specified module, run the **snmp-agent trap enable feature-name** *feature-name* **trap-name** *trap-name* command.
- To disable a specified trap for a specified module, run the **undo snmp-agent trap enable feature-name** *feature-name* **trap-name** *trap-name* command.
- To restore the default trap status of all modules, run the **undo snmp-agent trap disable** or **undo snmp-agent trap enable** command.

The **snmp-agent trap enable** command must be used together with the **snmp-agent target-host inform** command or **snmp-agent target-host trap** command.

To enable a device to send traps, you need to run at least the **snmp-agent target-host inform** command or **snmp-agent target-host trap** command on the device to specify the destination address of the traps.

Example

Enable the switch to send traps.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable
Warning: All switches of SNMP trap/notification will be open. Continue? [Y/N]:y
```

16.1.63 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.	acle, adpvxlan, arp, asmngtrap, bfd, bgp, cfgmgr, clkm, configuration, datasync, dhcp, dldp, easyoperatrap, efm, emdi, entityexttrap, entitymib, entitytrap, eoam-1ag, eoam-y1731, erps, error-down, etrunk, fm, ftp_server, gtl, hgmp, hsb-trap, http, ifnet, ifpdt, igmp, info, ip, ipfpm, iplpm, ipsec, ipv6, isis, l2bptnl, l2if, l2ifppi, l2vpn, l3mb, l3vpn, lacp, lbdt, ldp, line, lldptrap, loopdetect, mad, mcast, mid_aaa, mid_am, mid_eapol, mid_web, mld, mpls, mpls_lspm, mpls_rsvp, mrm, msdp, mstp, ntp, ospf, ospfv3, pim, pim-std, pki, pm, ptp, qose, radius, rip, rm, rmon, rrpp, securitytrap, sindex, snmp, srmtrap, sspadp, stack, swithsrvres, sysres, system, tcp, trunk, tunnel-te, uni-topomng, uni-tplm, uni-vermng, unimbrtrap, usbloadtrap, vbst, vcmp, vfs, vplsoam, vrrp, wlan
trap-name *trap-name*	Specifies the name of a trap.	For details about the alarm, see the Alarm Handling.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If **trap-name** *trap-name* is not specified, the switch 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 feature-name all** command to check the configuration result.

Precautions

- The feature name asmngtrap, uni-topomng, uni-tplm, uni-vermng, and unimbrtrap are supported only on the SVF parent.
- The feature name etrunk is supported only on the S5720I-SI, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H,

S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.

- The feature name igmp, mld, mrm, msdp, pim-std, and pim are supported only on the S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S.
- The feature name gtl takes effect only on the device that loads the license control item.
- If the IS-IS trap function is enabled before a version upgrade, you need to run the **snmp-agent trap enable feature-name isis** command to re-enable the trap function after the version upgrade. Otherwise, the previous configuration is lost.

Example

Enable the switch to send the fallingalarm trap about RMON to the NMS.

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

16.1.64 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 300 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 300.

Views

System view

Default Level

3: Management level

Usage Guidelines

Any trap messages are discarded after the duration expires. The trap messages are no longer reserved or sent.

Example

Set the lifetime of trap messages to 60 seconds.

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

16.1.65 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 1000.

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 1000.

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
```

16.1.66 snmp-agent trap start-trap resend disable

Function

The **snmp-agent trap start-trap resend disable** command disables the function of resending device cold-start or warm-start traps.

The **undo snmp-agent trap start-trap resend disable** command restores the default status of the function of resending device cold-start or warm-start traps.

By default, the function of resending device cold-start or warm-start traps is enabled.

Format

snmp-agent trap start-trap resend disable

undo snmp-agent trap start-trap resend disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

SNMP uses the resending mechanism for device cold-start or warm-start traps. This mechanism works in the following way:

- The system resends a cold-start or warm-start trap for three consecutive times to ensure that the trap can be sent to the destination.
- The first trap that the device sends must be a cold-start or warm-start trap. If another alarm is generated before the cold-start or warm-start trap, the system buffers that alarm and sends it only after the cold-start or warm-start trap is sent. The system also resends the buffered alarm for three consecutive times.

If the function of resending device cold-start or warm-start traps is not required any more, run the **snmp-agent trap start-trap resend disable** command to disable it.

Example

Disable the function of resending device cold-start or warm-start traps.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap start-trap resend disable
```

16.1.67 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.

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 VLANIF100 as the source address of traps.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap source vlanif 100
```

16.1.68 snmp-agent trap source-port

Function

The **snmp-agent trap source-port** command configures the number of the source port that sends trap messages.

The **undo snmp-agent trap source-port** command restores the default number of the source port that sends trap messages.

By default, the source port that sends trap messages is a random port.

Format

snmp-agent trap source-port *port-num*

undo snmp-agent trap source-port

Parameters

Parameter	Description	Value
port-num	Specifies the number of the source port that sends trap messages.	The value is an integer ranging from 1025 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve security of network packets, run the **snmp-agent trap source-port** command to configure the source port that sends trap messages. Therefore, the user firewall filters packets based on the port number.

Precautions

By default, a random port is used to send trap messages, and no configuration file is generated. After you configure a specific source port, the corresponding

configuration file is generated. If you delete the specified source port, no configuration file is generated.

If a device sends packets to the NMS in Inform mode and the **snmp-agent trap source-port** command is run to change the source port number, SNMP uses the new source port instead of the original port to receive response packets from the NMS. As a result, packets are retransmitted.

Example

Set the number of the source port that sends SNMP agent trap messages to **1057**.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap source-port 1057
```

16.1.69 snmp-agent trap type

Function

The **snmp-agent trap type** command configures the device to send ENTITYTRAP traps or BASETRAP traps.

The **undo snmp-agent trap type** command restores the default configuration.

By default, the device sends BASETRAP traps.

Format

snmp-agent trap type { **base-trap** | **entity-trap** }

undo snmp-agent trap type

Parameters

Parameter	Description	Settings
base-trap	Configures the device to send BASETRAP traps.	-
entity-trap	Configures the device to send ENTITYTRAP traps.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There are two types of traps for the hardware of the switch: BASETRAP and ENTITYTRAP.

- The BASETRAP traps are sent when faults occur, so they are classified based on fault types. For example, the same BASETRAP trap is sent when a Power Module or a fan is removed.
- The ENTITYTRAP traps are classified based on hardware types. For example, different ENTITYTRAP traps are sent when a Power Module is removed and when a fan is removed.

The functions of the two types of traps are similar. Select one type of traps based on your requirements.

Precautions

The following conditions must be met; otherwise, the device does not send BASETRAP traps to the NMS:

- The trap type is set to base-trap using the **snmp-agent trap type** command.
- The BASETRAP trap function is enabled.

The following conditions must be met; otherwise, the device does not send ENTITYTRAP traps to the NMS:

- The trap type is set to entity-trap using the **snmp-agent trap type** command.
- The ENTITYTRAP trap function is enabled.

You can run the **clear alarm active** command to clear the alarms that are generated before the alarm type is changed.

After NETCONF is enabled on a device, the device sends traps only based on entity-trap.

Example

Configure the device to send BASETRAP traps.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap type base-trap
```

16.1.70 snmp-agent udp-port

Function

The **snmp-agent udp-port** command sets the listening port of the SNMP agent.

The **undo snmp-agent udp-port** command restores the default listening port of the SNMP agent.

By default, the listening port of the SNMP agent is 161.

Format

snmp-agent udp-port *port-num*

undo snmp-agent udp-port

Parameters

Parameter	Description	Value
port-num	Specifies the listening port of the SNMP agent.	The value is 161 or an integer that ranges from 1025 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The SNMP agent is a proxy process running on a network device. By default, the SNMP agent listens on port 161 to respond to instructions sent from the NMS. In this manner, the NMS can manage the network device. Fixing the listing port may threaten network security. For example, if all attack packets are sent to this listening port, the network is congested.

To improve device security, run the **snmp-agent udp-port** command to change the listening port of the SNMP agent.

Configuration Impact

After you run this command, the SNMP agent listens on the new port number. The original SNMP connection with the NMS is torn down, and the NMS must use the new port number to connect to the device.

Precautions

- Before configuring the listening port of the SNMP agent, run the **snmp-agent protocol source-interface** or **snmp-agent protocol source-status** command to enable the network device to receive and respond to NMS request packets.
- The listening port configured on the NMS must be the same as that specified by the **snmp-agent udp-port** command. Otherwise, the NMS cannot connect to the device.

Example

Set the listening port of the SNMP agent to 1057.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent udp-port 1057
```

16.1.71 snmp-agent usm-user

Function

The **snmp-agent usm-user** command creates an SNMPv3 user.

The **undo snmp-agent usm-user** command deletes an SNMPv3 user.

By default, no SNMPv3 user exists on a device.

Format

snmp-agent [**remote-engineid** *engineid*] **usm-user v3** *user-name* [**group** *group-name* | **acl** { *acl-number* | *acl-name* }] *

snmp-agent [**remote-engineid** *engineid*] **usm-user v3** *user-name* **authentication-mode** { **md5** | **sha** | **sha2-256** } [**localized-configuration cipher** *password* | **cipher** *password*]

snmp-agent [**remote-engineid** *engineid*] **usm-user v3** *user-name* **privacy-mode** { **des56** | **aes128** | **aes192** | **aes256** | **3des** } [**localized-configuration cipher** *password* | **cipher** *password*]

snmp-agent [**remote-engineid** *engineid*] **usm-user v3** *user-name* **group** *group-name* **acl-ipv4** { *acl-number* | *acl-name* } [**acl-ipv6** { *acl-number* | *acl-name* }]

snmp-agent [**remote-engineid** *engineid*] **usm-user v3** *user-name* **group** *group-name* **acl-ipv6** { *acl-number* | *acl-name* }

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

Parameters

Parameter	Description	Value
remote-engineid *engineid*	Specifies the ID of the engine associated with a user. **remote-engineid** *engineid* must be set to the engine ID of the destination host that receives alarms. The engine IDs of the source and destination hosts must be different.	The value is string of 10 to 64 hexadecimal digits. It cannot be all 0s or all Fs.
v3	Indicates that the security mode in SNMPv3 is adopted.	-
user-name	Specifies the name of an SNMPv3 user.	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.

Parameter	Description	Value
group *group-name*	Specifies the SNMPv3 user group to which the SNMPv3 user belongs.	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.
authentication-mode	Sets the authentication mode. 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.	-
md5 | **sha** | **sha2-256**	Specifies the authentication algorithm. • **md5**: Specifies HMAC-MD5-96 as the authentication algorithm. • **sha**: Specifies HMAC-SHA-96 as the authentication algorithm. • **sha2-256**: Specifies HMAC-SHA2-256-192 as the authentication algorithm. **NOTE** For higher security purposes, you are advised to specify the **sha2-256** parameter.	-
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.	-

Parameter	Description	Value
des56 | **aes128** | **aes192** | **aes256** | **3des**	Specifies DES-56, AES-128, AES-192, AES-256, or 3DES as the encryption algorithm. **NOTE** For higher security purposes, the DES-56 or 3DES algorithm is not recommended. If the DES-56 or 3DES algorithm is used, do not use passwords composed of repeated character strings. For example, in *str***n*, *str* is a repeated character string and *n* indicates the number of times this string repeats. Otherwise, the passwords containing any times of *str* can pass authentication. For example, if the password is **Huawei@123Huawei@123**, passwords **Huawei@123Huawei@123**, and **Huawei@123Huawei@123Huawei@123** can all pass authentication.	-
localized-configuration	Specifies the localized password configuration mode. **NOTE** After authentication and encryption passwords are configured through MIB, this keyword is displayed in the commands recorded in configuration files. After authentication and encryption passwords are configured through command line, you are not advised to use this keyword. If this keyword is used, the cipher text passwords configured later use the local format. As a password with the **localized-configuration** keyword is related to the engine ID, copying configurations with this keyword from one device to another causes the password to be invalid.	-

Parameter	Description	Value
cipher *password*	Specifies the password.	The value is a case-insensitive string without spaces. It must be in cipher text format with 32 to 108 characters. • The password should not contain repeated character strings such as abc123abc123abc123 and **123abc**123abc. • The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character. Special characters do not include the question mark (?) and space. • The password entered in interactive mode is not displayed on the screen.
acl	Specifies an ACL that takes effect on both IPv4 and IPv6 networks.	-
acl-ipv4	Specifies an ACL that takes effect on only IPv4 network.	-
acl-ipv6	Specifies an ACL that takes effect on only IPv6 network.	-
acl-number	Specifies the number of an ACL.	The value is an integer ranging from 2000 to 3999.

Parameter	Description	Value
acl-name	Specifies the name of a basic or an advanced Named ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

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 encryption. SNMPv3 can provide higher security and confidentiality than SNMPv1 and SNMPv2c. The following table lists the difference between SNMPv1, SNMPv2c, and SNMPv3:

Table 16-21 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 SNMPv3 user group. The **snmp-agent group** command can be used to configure the rights for SNMPv3 users in a specified SNMPv3 user group and bind the SNMPv3 user 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 SNMPv3 user group is configured, the

MIB-view-based access control is configured for the SNMPv3 user group. Users cannot access objects in the MIB view through the SNMPv3 user group. The purpose of adding SNMPv3 users to an SNMPv3 user group is to ensure that SNMPv3 users in an SNMPv3 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 SNMPv3 user group, you configure the MIB-view-based access rights for the user. If an SNMPv3 user group is configured with the AuthPriv access rights, you can configure the authentication mode and encryption mode when configuring SNMPv3 users. Note that the authentication keys and encryption passwords configured on the NMS and the SNMP agent should be the same; otherwise, authentication fails.

To ensure that the NMS correctly receives the alarm in Inform mode sent by the switch, run the **snmp-agent remote-engineid** *engineid* **usm-user v3** *user-name* command to specify the NMS engine ID on the host. After the command is run, the host encapsulates the NMS engine ID in the Authoritative Engine ID field of the SNMPv3 alarm packet before sending the alarm in Inform mode. After receiving the alarm, the NMS compares the engine ID carried in the received packet with its own engine ID. If the two IDs match, the NMS sends a response to the alarm host. If the two IDs do not match, the NMS discards the packet.

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 security level of the SNMPv3 user must be higher than or equal to the security level of the SNMPv3 user group to which the SNMPv3 user belongs. The security level can be (in descending order): AuthPriv (authentication and encryption), authNoPriv (authentication without encryption), and noAuthNoPriv (neither authentication nor encryption). If the user security level is set to neither authentication nor encryption, the user only has the read-only permission within MIB-2 (OID: 1.3.6.1.2.1).

To add an SNMPv3 user to an SNMPv3 user group, ensure that the SNMPv3 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.

When a user with a level lower than the level configured using this command queries the password configured using the **display this** command, the password is displayed as asterisks (******).

To specify the same ACL on IPv4 and IPv6 networks, you can only run the **snmp-agent** [**remote-engineid** *engineid*] **usm-user v3** *user-name* **acl** { *acl-number* | *acl-name* } command.

If the **snmp-agent usm-user** command is run more than once to specify an ACL for the same SNMPv3 user, the latest configuration overrides the previous one.

Example

Configure an SNMPv3 user with user name **u1**, group name **g1**, authentication mode **sha2-256**, 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 sha2-256
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]
```

16.1.72 snmp-agent usm-user password complexity-check disable

Function

The **snmp-agent usm-user password complexity-check disable** command disables the complexity check for SNMPv3 user passwords.

The **undo snmp-agent usm-user password complexity-check disable** command enables the complexity check for SNMPv3 user passwords.

By default, the complexity check is enabled for SNMPv3 user passwords.

Format

snmp-agent usm-user password complexity-check disable

undo snmp-agent usm-user password complexity-check disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the complexity check is enabled for SNMPMv3 user passwords, a newly-configured SNMPv3 user password needs to meet the requirements for the complexity check. After complexity check is disabled for SNMPv3 user passwords, the complexity of the passwords is not checked.

The requirements for the complexity of SNMPv3 user passwords are as follows:

- The password cannot be the same as the user name and cannot be the same as the user name in reverse order.
- The minimum length of a password is configured by using the **set password min-length** command. By default, a password contains 8 characters at least.
- A password includes at least two kinds of characters: uppercase letters, lowercase letters, numbers, and special characters (excluding question marks (?) and spaces).

Precautions

- After complexity check is disabled for SNMPv3 user passwords, if a configured SNMPv3 user password is simple and does not meet the complexity requirements, the password may be easily attacked and cracked down by unauthorized users, affecting device security. Therefore, enabling the complexity check for SNMPv3 user passwords is recommended.
- In the configuration restoration stage, complexity check is not performed for SNMPv3 user passwords.
- Enabling the complexity check for SNMPv3 user passwords does not affect the SNMPv3 user passwords that have been configured.

Example

Disable the complexity check for SNMPv3 user passwords.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent usm-user password complexity-check disable
```

16.1.73 storage

Function

The **storage** command configures the storage mode for a bulk file.

The **undo storage** command restores the default storage mode for a bulk file.

By default, a bulk file is stored in ephemeral mode.

Format

storage ephemeral

undo storage

Parameters

Parameter	Description	Value
ephemeral	Indicates the ephemeral storage mode in which the bulk file is deleted after a specified period.	-

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

Currently, the device supports only the ephemeral storage mode, which is the default storage mode. This command can be upgraded to support more storage modes.

Example

Set the storage mode of the bulk file **iftable** to ephemeral.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] storage ephemeral
```

16.1.74 transfer

Function

The **transfer** command configures the method of uploading a statistics file.

The **undo transfer** command removes the configured statistics file uploading method.

By default, a statistics file is not uploaded.

Format

transfer { **primary** | **secondary** } **protocol** { **tftp** | { { **ftp** | **sftp** } **username** *user-name* **password** *password* } } { **host** *host-name* } [**path** *destination-path*]

undo transfer { **primary** | **secondary** }

Parameters

Parameter	Description	Value
primary	Indicates the primary method of uploading a statistics file.	-
secondary	Indicates the secondary method of uploading a statistics file.	-
protocol	Indicates the protocol used by uploading a statistics file.	-
tftp	Specifies uploading a statistics file using TFTP.	-
ftp	Specifies uploading a statistics file using FTP.	-
sftp	Specifies uploading a statistics file using SFTP.	-
username *user-name*	Specifies the user name for uploading a statistics file using FTP or SFTP.	The value is a string of 1 to 64 characters.
password *password*	Specifies the user password for uploading a statistics file using FTP or SFTP.	In plaintext mode, the value is a string of 1 to 16 characters. In ciphertext mode, the value is a string of 32 or 48characters.
host *host-name*	Specifies the host name of the server.	The value is a string of 1 to 20 characters.
path *destination-path*	Specifies the destination folder for uploaded files.	The value is a string of 1 to 64 characters.

Views

Bulk-file view

Default Level

2: Configuration level

Usage Guidelines

Primary and secondary methods of uploading statistics files are supported. If the primary method fails, the secondary method is adopted.

You must configure a primary before enabling a statistics file. The secondary is optional.

You can modify a primary or secondary but cannot delete a primary when a statistics file is enabled; however, you can delete or configure a secondary when a statistics file is enabled.

Using SFTP as the upload mode is recommended to enhance security.

Example

Configure a primary method of uploading the statistics file named **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] transfer primary protocol sftp username user password pwd host host-name path folder/bulkstat1
```

Configure a secondary method of uploading the statistics file named **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] transfer secondary protocol tftp host 10.1.0.1 path folder/bulkstat2
```

Remove the configured secondary method of uploading the statistics file named **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] undo transfer secondary
```

16.1.75 transfer interval

Function

The **transfer interval** command sets the upload interval for a bulk file.

The **undo transfer interval** command restores the default upload interval for a bulk file.

By default, the upload interval for a bulk file is 5 minutes.

Format

transfer interval *interval*

undo transfer interval

Parameters

Parameter	Description	Value
interval	Specifies the upload interval for a bulk file.	The value can be 5, 10, 15, or 30, in minutes.

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

The upload interval for a bulk file must be longer than or equal to the statistics collection interval of the bulk file, and is an integral multiple.

The upload interval for a bulk file can be changed only when the bulk file is disabled.

Example

Set the upload interval to 15 minutes for the bulk file **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] transfer interval 15
```

16.1.76 transfer remain-time

Function

The **transfer remain-time** command sets the upload holding time for a bulk file.

The **undo transfer remain-time** command restores the default upload holding time for a bulk file.

By default, the upload holding time for a bulk file is 5 minutes.

Format

transfer remain-time *remain-time*

undo transfer remain-time

Parameters

Parameter	Description	Value
remain-time	Specifies the upload holding time for a bulk file.	The value is an integer that ranges from 1 to 30, in minutes.

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an upload interval expires, the compressed bulk file must be retained for a period to ensure enough time for the file to be uploaded. This period is the upload holding time.

When the network quality is high and the file transfer is fast, you can reduce the upload holding time. When the network quality is low and the file transfer is slow, increase the upload holding time to improve file transfer reliability.

Precautions

To ensure that only one copy of a bulk file is uploaded to the server, set *remain-time* to be smaller than or equal to the file upload interval.

Example

Set the upload holding time to 10 minutes for bulk file **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] transfer remain-time 10
```

16.1.77 transfer retry

Function

The **transfer retry** command sets the maximum number of retransmissions for a bulk file.

The **undo transfer retry** command restores the default maximum number of retransmissions for a bulk file.

By default, the maximum number of retransmissions for a bulk file is 5.

Format

transfer retry *retry-times*

undo transfer retry

Parameters

Parameter	Description	Value
retry-times	Specifies the maximum number of retransmissions for a bulk file.	The value is an integer that ranges from 0 to 5.

Views

Bulk file view

Default Level

2: Configuration level

Usage Guidelines

The maximum number of retransmissions for a bulk file can be changed only when the bulk file is disabled.

If *retry-times* is set to 0 for a bulk file, the system does not retransmit the bulk file when the file fails to be uploaded.

Example

Set the maximum number of retransmissions to 1 for the bulk file **iftable**.

```
<HUAWEI> system-view
[HUAWEI] bulk-stat enable
Info: Succeeded in enabling the bulk stat function.
[HUAWEI] bulk-file iftable
[HUAWEI-bulk-file-iftable] transfer retry 1
```

16.2 RMON and RMON2 Configuration Commands

16.2.1 Command Support

All models of S300, S500, S2700, S5700, and S6700 series switches (except the S5731-L and S5731S-L) support RMON and RMON2.

16.2.2 display rmon alarm

Function

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

Format

display rmon alarm [*entry-number*]

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
```

Table 16-22 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(no valid trap). You can run the **rmon alarm** command to configure *entry-number* and *owner*.

Item	Description
Samples delta value	Alarm variable, namely, monitored MIB object, corresponding to the alarmVariable object in alarmTable. You can run the **rmon alarm** command to configure this parameter.
Sampling interval	Sampling interval, in seconds, corresponding to the alarmInterval object in alarmTable. You can run the **rmon alarm** command to configure this parameter.
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. You can run the **rmon alarm** command to configure this parameter.
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. You can run the **rmon alarm** command to configure this parameter.
When startup enables	Condition that triggers alarms for the first time, 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 You can run the **rmon alarm** command to configure this parameter.
Latest value	Latest sampled value, corresponding to the alarmValue object in alarmTable.

16.2.3 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

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 Test is valid.
  Description: null.
  Will cause log  when triggered, last triggered at 0days 00h:24m:10s.69th.
```


Table 16-23 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(no valid event). You can run the **rmon event** command to configure *entry-number* and *owner*.
Description	Event description, corresponding to the eventDescription object in eventTable. You can run the **rmon event** command to configure this parameter.
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. You can run the **rmon event** command to configure this parameter.
last triggered at	Latest event time, corresponding to the eventLastTimeSent object in eventTable.

16.2.4 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

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 16-24 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(no valid event log).
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.

16.2.5 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     : GigabitEthernet0/0/1<ifIndex.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 gigabitethernet 0/0/1
History control entry 1 owned by Creator is valid
  Samples interface     : GigabitEthernet0/0/1<ifIndex.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 16-25 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(no valid historical sampling information). You can run the **rmon history** command to configure *entry-number* and *owner*.
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. You can run the **rmon history** command to configure this parameter.
Last Sampling time	Latest sampling time, corresponding to the etherHistoryIntervalStart object in etherHistoryTable.
Latest sampled values	Latest sampling result.
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.

Item	Description
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.
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.

16.2.6 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.

Example

Display the RMON extended alarm configurations.

```
<HUAWEI> display rmon prialarm
Prialarm table 1 owned by Test 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 16-26 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 index. • *owner*: creator of the entry. • *status*: row status of the extended alarm entry with the specified index: undercreation(invalid), valid(valid), invalid(no valid extended alarm information). You can run the **rmon prialarm** command to configure *entry-number* and *owner*.
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. You can run the **rmon prialarm** command to configure this parameter.

Item	Description
Sampling interval	Interval at which traffic is sampled, in seconds. You can run the **rmon prialarm** command to configure this parameter.
Rising threshold	Alarm rising threshold. You can run the **rmon prialarm** command to configure this parameter.
Falling threshold	Alarm falling threshold. You can run the **rmon prialarm** command to configure this parameter.
linked with event *entry-number*	Associate with the row with index *entry-number*. You can run the **rmon prialarm** command to configure this parameter.
When startup enables	Condition that triggers alarms for the first time. 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 You can run the **rmon alarm** command to configure this parameter.
This entry will exist	Aging time of the extended alarm entry. An entry may be valid permanently or in a certain period. You can run the **rmon prialarm** command to configure this parameter.
Latest value	Latest sampling result.

16.2.7 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

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 : GigabitEthernet0/0/1<ifIndex.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 16-27 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(no valid statistics information). You can run the **rmon statistics** command to configure *entry-number* and *owner*.
Interface	Interface where statistics are collected, corresponding to the etherStatsDataSource object in etherStatsTable, followed by the interface OID.
Received	Number of received packets.
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. **NOTE** The SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S cannot collect statistics on the packets of which the lengths range from 1518 to **n**. **n** is the maximum frame length allowed by the interface, and can be set using the **jumboframe enable** command.
fragments packets	Number of received undersize and CRC error packets, corresponding to the etherStatsFragments object in etherStatsTable.

Item	Description
jabbers packets	Number of received large and CRC error packets, corresponding to the etherStatsJabbers object in etherStatsTable. **NOTE** The S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S do not support this item.
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. **NOTE** In classified packet statistics on the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S, 1024-1518 includes the packets longer than 1518. On the S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, S5736-S, or S6720S-S, this field is displayed 0.

16.2.8 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
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
maxentries - hlhostcontrolnlmaxdesiredentries
status - hlhostcontrolstatus

index datasource              droppedfrm inserts    Deletes    maxentries      status
123   Vlanif10                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 :   Vlanif10
droppedfrm :   0
inserts    :   0
Deletes    :   0
```



```
maxentries :  50
owner      :  china
status     :  active
```

Table 16-28 Description of the **display rmon2 hlhostcontroltable** command output

Item	Description
index	Index of an entry in the hlHostControlTable. You can run the **rmon2 hlhostcontroltable** command to configure this parameter.
datasource	Source interface of data. You can run the **rmon2 hlhostcontroltable** command to configure this parameter.
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 hlHostControlTable contains. You can run the **rmon2 hlhostcontroltable** command to configure this parameter.
owner	Owner of the entry in the hlHostControlTable. You can run the **rmon2 hlhostcontroltable** command to configure this parameter.
status	Status of the entry in the hlHostControlTable: ● active: running normally ● not in service: invalid You can run the **rmon2 hlhostcontroltable** command to configure this parameter.

16.2.9 display rmon2 nlhosttable

Function

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

Format

display rmon2 nlhosttable [**hostcontrolindex** *ctrl-index*] [**timemark** *time-value*] [**protocoldirlocalindex** *protocol-local-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.
timemark *time-value*	Enables the time filter.	The value is in the range of 0 to 4294967295. The entries in the nlHostTable with the ChgTm value being larger than this value are displayed.
protocoldirlocalindex *protocol-local-index*	Identifies the network layer protocol of the nlHostAddress.	Its value ranges from 1 to 2147483647.
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 protocoldirlocalindex 2 hostaddress
10.110.94.177
Abbreviation:
HIdx - hlHostControlIndex
PIdx - ProtocolDirLocalIndex
Addr - nlHostAddress
InPkts - nlHostInPkts
OutPkts - nlHostOutPkts
InOctes - nlHostInOctets
OutOctes - nlHostOutOctets
OutMac - nlHostOutMacNonUnicastPkts
ChgTm - nlHostTimeMark
CrtTm - nlHostCreateTime
HIdx  PIdx Addr          InPkts  OutPkts InOctes OutOctes OutMac        ChgTm                       CrtTm
1     2    10.110.94.177 59      68      3240    3821     0         0 days 00h:01m:29s.09th(8909)  0 days 00h:
01m:01s.13th(6113)
```


Table 16-29 Description of the display rmon2 nlhosttable command output

Item	Description
HIdx	Index of the host control table.
PIdx	Protocol directory index.
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.
ChgTm	Entry time filter in the host control table.
CrtTm	Customized time filter.

16.2.10 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

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           :  ww
protocolDirAddressMapConfig:  not supported
protocolDirHostConfig      :  supported on
protocolDirMatrixConfig    :  not supported
protocolDirOwner           :  test
protocolDirStatus          :  active
```

Table 16-30 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	Indicates the description of the protocol directory table. You can run the **rmon2 protocoldirtable** command to configure this parameter.
protocolDirAddress-MapConfig	Whether protocol directory address mapping is supported. This function is not supported currently.
protocolDirHostConfig	Whether the configuration of protocol directory host is supported: ● not supported: The device does not monitor the network-layer host table of the protocol, and this value cannot be changed. ● supported on: The device can monitor the network-layer host table of the protocol, and the monitoring function is enabled. ● supported off: The device can monitor the network-layer host table of the protocol, but the monitoring function is disabled. You can run the **rmon2 protocoldirtable** command to configure this parameter.

Item	Description
protocolDirMatrixConfig	Whether protocol directory matrix is supported. This function is not supported currently.
protocolDirOwner	Indicates the owner. You can run the **rmon2 protocoldirtable** command to configure this parameter.
protocolDirStatus	Protocol directory status. • active: running normally • not in service: invalid You can run the **rmon2 protocoldirtable** command to configure this parameter.

16.2.11 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* [**startup-alarm** { **falling** | **rising** | **risingorfalling** }] [**owner** *owner-name*]

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 OID of a monitored object.	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.

Parameter	Description	Value
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.

Parameter	Description	Value
startup-alarm { **falling** | **rising** | **risingorfalling** }	Specifies the condition of sending an alarm when the system data is sampled for the first time. • **falling**: an alarm is sent when the sampled value falls below the lower threshold value. • **rising**: an alarm is sent when the sampled value exceeds the upper threshold value. • **risingorfalling**: an alarm is sent when the sampled value exceeds the upper threshold value or the lower threshold value. **NOTE** An alarm is sen no matter whether the following sampled value exceeds the upper threshold value or the lower threshold value.	-
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.

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 greater 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. Otherwise, events cannot be triggered even if alarms are generated.

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 the alarm threshold of etherStatsBroadcastPkts.1 (1.3.6.1.2.1.16.1.1.1.6.1) and sample the absolute value with an interval of 30 seconds. When the sampled value is greater than or equal to the upper threshold 500, event 1 is triggered. When the sampled value is less than or equal to the lower threshold 100, event 2 is triggered. The **creator** parameter indicates the owner that creates the event.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] rmon statistics 1 owner creator
[HUAWEI-GigabitEthernet0/0/1] 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
```

16.2.12 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

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
```

16.2.13 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.
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 interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE 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.

In versions earlier than V200R019C00, this command cannot be configured on Eth-Trunk member interfaces. Starting from V200R019C00, this command can be configured on Eth-Trunk member interfaces.

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 gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] rmon history 1 buckets 10 interval 5 owner user1
```

16.2.14 rmon prialarm

Function

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

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.

Parameter	Description	Value
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.
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.

Parameter	Description	Value
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.

Situation	Action
The sampled value is greater 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 **Test**.

```
<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 Test
```

16.2.15 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*

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 interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE 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.

Precautions

In versions earlier than V200R019C00, this command cannot be configured on Eth-Trunk member interfaces. Starting from V200R019C00, this command can be configured on Eth-Trunk member interfaces.

Example

Configure a statistics table on GigabitEthernet0/0/1 and add an entry with index 20 to the table.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] rmon statistics 20 owner creater
```

16.2.16 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.	-
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 gigabitethernet 0/0/1 maxentry 100 owner test status active
```

Set the hlHostControlStatus value in the host control table to **inactive**.

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

16.2.17 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
protocoldirid *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 { **notsupported** | **supportedon** | **supportedoff** }	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. • **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.

Parameter	Description	Value
status { **active** | **inactive** }	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.
  - 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 test host supportedon owner test 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 supportedoff.

```
<HUAWEI> system-view
[HUAWEI] rmon2 protocoldirtable protocoldirid 8.0.0.0.1.0.0.8.0 parameter 2.0.0 host supportedoff
```

16.2.18 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, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Port-Group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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

Precautions

In versions earlier than V200R019C00, this command cannot be configured on Eth-Trunk member interfaces. Starting from V200R019C00, this command can be configured on Eth-Trunk member interfaces.

After the interface mode is changed from Layer 2 to Layer 3 by using the **undo portswitch** command, the device does not support the **rmon-statistics enable** command.

Example

Enable RMON statistics function on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] rmon-statistics enable
```

16.3 LLDP Configuration Commands

16.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.3.2 cdp clear neighbor

Function

The **cdp clear neighbor** command clears CDP neighbors in the system or on an interface of the device.

Format

cdp clear neighbor [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Indicates the type and number of the interface whose CDP neighbors are to be cleared. In the command: ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface. If no interface is specified, this command clears CDP neighbors on all interfaces.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want to obtain the latest CDP neighbor information of interfaces, use the **cdp clear neighbor** command to clear existing CDP neighbors. When an interface receives new CDP packets, new CDP neighbors are generated.

Prerequisites

The LLDP function has been enabled globally and on interfaces, and the **lldp compliance cdp receive** command has been run to enable CDP-compatible LLDP on interfaces.

Example

Clear CDP neighbors on all the interfaces.

```
<HUAWEI> cdp clear neighbor
Warning: This command will clear CDP neighbor information of all the ports. Continue? [Y/N]:y
```


16.3.3 display cdp local

Function

The **display cdp local** command displays local CDP information on a specified interface or all interfaces.

Format

display cdp local [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the CDP local information on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, the command displays CDP local information on all the interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check CDP information on a specified interface or all interfaces, run the **display cdp local** information.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command, and LLDP compatibility with CDP has been enabled on the specified interface using the **lldp compliance cdp receive** command.

Example

Display CDP local information on all the interfaces.

```
<HUAWEI> display cdp local
Remote Table Statistics:
------------------------------------------------------------------------------
Remote Table Last Change Time   :0 days, 23 hours, 21 minutes, 37 seconds
Remote Neighbors Added          :0
Remote Neighbors Deleted        :0
```



```
Remote Neighbors Dropped       :0
Remote Neighbors Aged          :0
Total Neighbors                :1

Port information:
--------------------------------------------------------------------------------
Interface GigabitEthernet0/0/1:
CDP Status              :enabled            (default is disabled)
Total Neighbors         :1
Interface GigabitEthernet0/0/2:
CDP Status              :enabled      (default is disabled)
Total Neighbors         :0
  ---- More ----
```

Table 16-31 Description of the **display cdp local** command output.

Item	Description
Remote Table Statistics	Statistics about CDP neighbors.
Remote Table Last Change Time	Time of the latest update of the CDP neighbor table.
Remote Neighbors Added	Number of added CDP neighbors.
Remote Neighbors Deleted	Number of deleted CDP neighbors.
Remote Neighbors Dropped	Number of CDP neighbors that are deleted because of insufficient storage memory.
Remote Neighbors Aged	Number of CDP neighbors that are deleted by the aging mechanism.
Total Neighbors	Total number of CDP neighbors.
Port information	Local CDP information on all interfaces of the switch.
Interface *x*	Local CDP information on the *x* interface.
CDP Status	Whether LLDP compatibility with CDP is enabled on the interface: • enabled • disabled You can run the **lldp compliance cdp receive** command to configure this parameter.
Total Neighbors	Total number of CDP neighbors on the interface.

16.3.4 display cdp neighbor

Function

The **display cdp neighbor** command displays information about CDP neighbors of all interfaces or a specified interface.

Format

display cdp neighbor [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about CDP neighbors of a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, the command displays information about CDP neighbors of all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command enables you to know which CDP neighbors the local device has, Layer 2 information about the neighbors, and to which interfaces the neighbors connect. You can also use this command to check whether the Layer 2 information is configured correctly on the neighbors.

Prerequisites

LLDP has been enabled globally using the **lldp enable** command, and LLDP compatibility with CDP has been enabled on the specified interface using the **lldp compliance cdp receive** command.

Example

Display information about CDP neighbors of all the interfaces.

```
<HUAWEI> display cdp neighbor
GigabitEthernet0/0/1 has 1 neighbor(s):
```



```
Neighbor index :1
Device ID              :ME3400
Port ID               :GigabitEthernet0/4
Version               :SCCP75.8-3-3SR2S
Platform               :cisco ME-3400EG-2CS-A
Capabilities           :host
MacAddress               :b4a4-e3cf-e984
Discovered time          :0 days, 22 hours, 33 minutes, 36 seconds
Expired time           :122 s
Power drawn             :12000 mw
Power request ID        :39308
Power management ID     :2
Power request levels    :12000 mw 0 mw
 ---- More ----
```

Table 16-32 Description of the **display cdp neighbor** command output

Item	Description
m has *n* neighbor(s)	The interface *m* has *n* CDP neighbors.
Neighbor index	Index of a CDP neighbor.
Device ID	ID of the CDP neighbor.
Port ID	Interface of the CDP neighbor connecting to the switch.
Version	Version of the CDP neighbor.
Platform	Software platform of the CDP neighbor.
Capabilities	Type of the CDP neighbor: ● router ● trans-bridge ● switch ● host ● igmp ● repeater ● phone ● other
MacAddress	MAC address of the CDP neighbor.
Discovered time	Time when the CDP neighbor was discovered, that is, the time difference between the system time when the device discovers the CDP neighbor and the startup time of the switch.
Expired time	The aging time remaining of CDP neighbor, in seconds.
Power drawn	Power set on the source.
Power request ID	Requested power ID.
Power management ID	ID used to manage power. The ID is the number of times the power is changed.

Item	Description
Power request levels	Requested power level. The maximum power among the negotiated power values is selected.

16.3.5 display cdp neighbor brief

Function

The **display cdp neighbor brief** command displays brief information about CDP neighbors of the device.

Format

display cdp neighbor brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to quickly view brief information about CDP neighbors connected to a switch, such as CDP neighbor names and interfaces on which CDP neighbor relationships are set up.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command, and LLDP compatibility with CDP has been enabled on the specified interface using the **lldp compliance cdp receive** command.

Example

Display brief information about CDP neighbors.

```
<HUAWEI> display cdp neighbor brief
Local Intf      Neighbor Dev        Neighbor Intf       Exptime(s)
GE0/0/1         ME3400              GE0/0/4             144
```


Table 16-33 Description of the **display cdp neighbor brief** command output

Item	Description
Local Intf	Local interface of the switch that sets up a CDP neighbor relationship with a peer device.
Neighbor Dev	Name of a CDP neighbor. If the name of an LLDP neighbor contains more than 24 characters, only the first 21 characters plus an ellipsis (...) are displayed. This display format cannot be changed. For example, if the name of an LLDP neighbor is **Huawei123456789123456789123456789**, this field is displayed **Huawei123456789123456...**.
Neighbor Intf	Interface of a peer device that sets up a CDP neighbor relationship with the switch.
Exptime(s)	Time left before a CDP neighbor relationship expires, in seconds.

16.3.6 display cdp neighbor device-id

Function

The **display cdp neighbor device-id** command displays the name of a CDP neighbor.

Format

display cdp neighbor device-id

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the name of a CDP neighbor contains more than 24 characters, the **display cdp neighbor brief** command cannot display the complete name of the CDP neighbor. In this case, run the **display cdp neighbor device-id** command instead.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command, and LLDP compatibility with CDP has been enabled on the specified interface using the **lldp compliance cdp receive** command.

Example

Display the name of a CDP neighbor.

```
<HUAWEI> display cdp neighbor device-id
Local Interface  Neighbor Interface  Neighbor Device
GE0/0/3          GE0/0/1             Edge1i-11111111111111111111111111111111111111111111111
```

Table 16-34 Description of the **display cdp neighbor device-id** command output

Item	Description
Local Interface	Local interface of the switch that sets up a CDP neighbor relationship with a peer device.
Neighbor Interface	Interface of a peer device that sets up a CDP neighbor relationship with the switch.
Neighbor Device	Name of a CDP neighbor. A maximum of 255 characters can be displayed in this field.

16.3.7 display cdp statistics

Function

The **display cdp statistics** command displays statistics about CDP packets received.

Format

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

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about CDP packets received by a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, the command displays statistics about CDP packets received by all the interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When you need to locate an LLDP fault on a switch according to statistics about CDP packets received, run the **display cdp statistics** command.

NOTE

To check statistics about CDP packets received in a specified period of time, run the **reset cdp statistics** command to clear the historical CDP packet statistics. Wait for the specified period of time, and then run the **display cdp statistics** command to check the new CDP packet statistics.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command, and LLDP compatibility with CDP has been enabled on the specified interface using the **lldp compliance cdp receive** command.

Example

Display statistics about CDP packets received by all interfaces.

```
<HUAWEI> display cdp statistics
CDP statistics global Information:
Statistics for GigabitEthernet0/0/1:
Total frames received:    30
Total frames discarded:   0
Total frames error:       0
Last cleared time:        never
 ---- More ----
```

Table 16-35 Description of the **display cdp statistics** command output

Item	Description
CDP statistics global Information	Statistics about CDP packets received by the switch.
Statistics for *x*	Statistics about CDP packets received by the *x* interface.
Total frames received	Number of received CDP packets by this interface.
Total frames discarded	Number of discarded CDP packets by this interface.
Total frames error	Number of received CDP error packets by this interface.

Item	Description
Last cleared Time	Time when the statistics about CDP packets received on this interface are cleared last time: • If the statistics about CDP packets on this interface have been cleared, the time is displayed. • If the statistics about CDP packets on this interface have never been cleared, **never** is displayed.

16.3.8 display lldp device-classifier information

Function

The **display lldp device-classifier information** command displays LLDP neighbor information on a switch.

Format

display lldp device-classifier information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If a switch has multiple types of LLDP neighbors and needs to deliver different configurations to different types of LLDP neighbors, configure the Python script in advance and run the **lldp device-classifier enable** command to enable the switch to automatically execute the Python script after the LLDP neighbor changes. If the switch detects that a specified type of LLDP neighbor is added or deleted on an interface, the switch automatically delivers the predefined configuration in the Python script, reducing the configuration workload. You can run the **display lldp device-classifier information** command to view LLDP neighbor information on the switch, including the LLDP neighbor type.

Prerequisites

The **lldp device-classifier enable** command has been executed to enable the switch to automatically execute the Python script after the LLDP neighbor changes.

Example

Display LLDP neighbor information on a switch.

```
<HUAWEI> display lldp device-classifier information
Capability codes:
   (T) Telephone, (B) Bridge, (R) Router
   (W) WLAN Access Point, (O) Other

Local Intf    Trigger Source    Capability      Exptime(s)
GE0/0/1        LLDP Packet       B,R            149
GE0/0/2        LLDP Packet       B,R            120
```

Table 16-36 Description of the **display lldp device-classifier information** command output

Item	Description
Capability codes/Capability	LLDP neighbor type: • (T) Telephone: IP phone • (B) Bridge: switch • (R) Router: router • (W) WLAN Access Point: AP • (O) Other: others
Local Intf	Interface of the switch that detects the LLDP
Trigger Source	Method used by the switch to detect the LLDP neighbor • LLDP Packet: through LLDP packets. • CDP Packet: through CDP packets. The **lldp compliance cdp receive** command must have been executed to enable CDP-compatible LLDP on the interface.
Exptime(s)	Remaining time of the LLDP neighbor on the switch, in seconds

16.3.9 display lldp local

Function

The **display lldp local** command displays the global LLDP information or the LLDP information on a specified interface.

Format

display lldp local [**interface** *interface-type interface-number*]

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 an interface includes the interface information and MED interface information.

To verify the LLDP information and Layer 2 information of the system and interfaces, run this command.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Example

Display the global LLDP information, S5735-S24T4X is used as an example.

```
<HUAWEI> display lldp local
System information
--------------------------------------------------------------------------------
Chassis type   :MAC address
Chassis ID     :00e0-11fc-1710
System name    :HUAWEI
```



```
System description  :Huawei Switch S5735-S24T4X
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (S5720 V200R023C00)
Copyright (C) 2000-2019 HUAWEI TECH Co., Ltd.
System capabilities supported   :bridge router
System capabilities enabled     :bridge router
LLDP Up time   :2023-02-28 11:53:20

MED system information
--------------------------------------------------------------------------------
Device class   :Network Connectivity
(MED inventory information of master board)
HardwareRev       :VER.B
FirmwareRev       :NA
SoftwareRev       :Version 5.170 V200R023C00
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

System configuration
--------------------------------------------------------------------------------
LLDP Status                    :enabled            (default is enabled)
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:000b-09e6-3da1

Remote Table Statistics:
--------------------------------------------------------------------------------
Remote Table Last Change Time   :0 days, 0 hours, 4 minutes, 15
seconds
Remote Neighbors Added          :5
Remote Neighbors Deleted        :0
Remote Neighbors Dropped        :0
Remote Neighbors Aged           :0
Total Neighbors                 :5

Port information:
--------------------------------------------------------------------------------
Interface GigabitEthernet0/0/1:
LLDP Enable Status      :enabled            (default is enabled)
Total Neighbors         :1

Port ID subtype     :Interface name
Port ID             :GigabitEthernet0/0/1
Port description    :GigabitEthernet0/0/1

Port and protocol VLAN ID(PPVID)   :0
Port and protocol VLAN supported   :No
Port and protocol VLAN enabled     :No
Port VLAN ID(PVID)  :1
VLAN name of VLAN 1:VLAN 0001
VLAN name of VLAN 3:VLAN 0003
VLAN name of VLAN 4:VLAN 0004
Protocol identity   :STP RSTP/MSTP LACP EthOAM CFM

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(1000)/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       :1526

EEE support              :Yes
Transmit Tw              :16
Receive Tw               :16
Fallback Receive Tw      :65535
Echo Transmit Tw         :16
Echo Receive Tw          :16

MED port information

Media policy type   :Unknown
Unknown Policy      :Yes
VLAN tagged         :No
Media policy VlanID          :0
Media policy L2 priority     :0
Media policy Dscp            :0

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0.2(w)

 ---- More ----
```

Table 16-37 Description of the **display lldp local** command output.

Item	Description
System information	Global LLDP information.
Chassis type	Type of the Device ID: • Chassis component: chassis alias • Interface alias: interface alias • Port component: interface or backplane alias • MAC address: MAC address • Network address: network address • Interface name: name of the interface • Locally assigned: name of the local device
Chassis ID	Device ID.
System name	Name of the device.
System description	Description of the device.
Huawei Versatile Routing Platform Software	-
VRP (R) software, Version	Versions of the VRP and the software of the device.
Copyright (C) 2000-2013 HUAWEI TECH Co., Ltd.	Huawei copyright.

Item	Description
System capabilities supported	Capabilities supported of the local device, including: • bridge: bridge device • router: router
System capabilities enabled	Capabilities enabled on the local device.
LLDP Up time	Time when LLDP is enabled.
MED system information	MED TLV information of the device.
Device class	Type of the device.
MED inventory information of master board	-
HardwareRev	Hardware version of the device.
FirmwareRev	Firmware version of the device.
SoftwareRev	Software version of the device.
SerialNum	Serial number of the device. **NOTE** If the decimal value of a serial number is not in the range of 32 to 126, the serial number is displayed in octal notation.
Manufacturer name	Name of the manufacturer.
Model name	Name of a model.
Asset tracking identifier	Asset tracking ID.
System configuration	Global LLDP configuration.
LLDP Status	Whether LLDP is enabled globally on the switch: • Enabled • Disabled You can run the **lldp enable (system view)** command to configure this parameter.
default is *x*	Default value *x*.
LLDP Message Tx Interval	Interval for sending LLDP packets of the device, in seconds. You can run the **lldp message-transmission interval** command to configure this parameter.

Item	Description
LLDP Message Tx Hold Multiplier	Hold time multiplier of local device information stored on neighbors. You can run the **lldp message-transmission hold-multiplier** command to configure this parameter.
LLDP Refresh Delay	Delay in re-enabling the LLDP function on the switch, in seconds. You can run the **lldp restart-delay** command to configure this parameter.
LLDP Tx Delay	Delay in sending LLDP packets on the switch, in seconds. You can run the **lldp message-transmission delay** command to configure this parameter.
LLDP Notification Interval	Delay in sending the neighbor change traps to the NMS on the switch, in seconds. You can run the **lldp trap-interval** command to configure this parameter.
LLDP Notification Enable	Whether the function of sending LLDP traps to the NMS is enabled on the switch: • enabled • disabled You can run the **snmp-agent trap enable feature-name lldptrap** command to configure this parameter.
Management Address	LLDP management address of the switch. You can run the **lldp management-address** command to configure this parameter. If an invalid management address is used, the inactive field is added for this address. For example, if 10.1.1.1 is an invalid management address, the displayed information is as follows: Management Address :IP:10.10.10.1, 10.1.1.1 (inactive) MAC: 000b-09e6-3da1
Remote Table Statistics	Statistics about LLDP neighbors.
Remote Table Last Change Time	Time that elapsed since the latest modification of remote data.
Remote Neighbors Added	Number of added LLDP neighbors.
Remote Neighbors Deleted	Number of deleted LLDP neighbors.
Remote Neighbors Dropped	Number of devices that do not set up LLDP neighbor relationships because the number of neighbors has reached the maximum value.

Item	Description
Remote Neighbors Aged	Number of LLDP neighbors that are aged out and deleted.
Total Neighbors	Number of LLDP neighbors.
Port information	LLDP information on the interface.
LLDP Enable Status	Whether LLDP is enabled on the interface: • Enabled • Disabled You can run the **lldp enable (system view)** and **lldp enable (interface view)** commands to configure this parameter.
Total Neighbors	Number of LLDP neighbors on the interface.
Port ID subtype	Type of the interface ID. • Interface alias: interface alias • Port component: interface or backplane alias • MAC address: MAC address • Network address: network address • Interface name: name of the interface • Agent circuit ID: circuit ID of the DHCP agent • Locally assigned: name of the local device
Port ID	Interface ID.
Port description	Interface description.
Port and protocol VLAN ID(PPVID)	Protocol VLAN ID of a port.
Port and protocol VLAN supported	Whether PPVID is supported: • Yes: PPVID is supported. • No: PPVID is not supported.
Port and protocol VLAN enabled	Whether PPVID is enabled: • Yes: PPVID is enabled. • No: PPVID is disabled.
Port VLAN ID(PVID)	The default VLAN ID of the interface.
VLAN name of VLAN 1 VLAN name of VLAN 3 VLAN name of VLAN 4	Name of a VLAN to be advertised, which is configured using the **lldp tlv-enable dot1-tlv** command. If no VLAN name is specified, the default VLAN name is advertised and displayed.
Protocol identity	Protocol ID.

Item	Description
Auto-negotiation supported	Whether the interface supports auto-negotiation: ● Yes ● No
Auto-negotiation enabled	Whether the interface is enabled with auto-negotiation: ● Yes ● No You can run the **negotiation auto** command to configure this parameter.
OperMau	Rate and duplex mode of the interface.
Power port class	PoE type of the interface: ● 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
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.

Item	Description
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. You can run the **jumboframe enable** command to configure this parameter.
EEE support	Whether the interface supports energy efficient Ethernet (EEE): ● Yes ● No
Transmit Tw	Amount of time the sender waits before starting sending data after leaving lower power consumption mode (LPI mode).
Receive Tw	Amount of time the receiver expects the sender to wait before starting sending data after leaving LPI mode.
Fallback Receive Tw	Additional information provided to the sender.
Echo Transmit Tw	Transmit Tw value specified in the Echo message sent from the remote end.
Echo Receive Tw	Receive Tw value specified in the Echo message sent from the remote end.
MED port information	-

Item	Description
Media policy type	Type of the media policy: ● Voice ● Voice Signaling ● Guest Voice ● Guest Voice Signaling ● Softphone Voice ● Video Conferencing ● Streaming Video ● Video Signaling ● Unknown
Unknown Policy	Whether the type of the media policy is unknown: ● Yes: unknown ● Defined: known ● Unknown indicates that the Media policy VlanID, Media policy L2 priority and Media policy Dscp value fields are ignored.
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	802.1p priority.
Media policy Dscp	DSCP value.
Power Type	Power supply type: ● PSE: power-sourcing equipment ● PD: powered device ● Unknown: an unknown power supply type Layer 3 interfaces do not support PoE TLV, so this parameter is not displayed on Layer 3 interfaces.
PoE PSE power source	Type of the PSE: ● Primary: indicates primary power supply. ● Backup: indicates backup power supply. ● Unknown: indicates an unknown type of PSE. Layer 3 interfaces do not support PoE TLV, so this parameter is not displayed on Layer 3 interfaces.

Item	Description
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. Layer 3 interfaces do not support PoE TLV, so this parameter is not displayed on Layer 3 interfaces.
Port Available power value	Port power supply. Layer 3 interfaces do not support PoE TLV, so this parameter is not displayed on Layer 3 interfaces.

16.3.10 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*]

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

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Example

Display information about neighbor devices of interfaces GigabitEthernet0/0/1. (The neighbor is a switch.)

```
<HUAWEI> display lldp neighbor interface gigabitethernet0/0/1
GigabitEthernet0/0/1 has 1 neighbor(s):

Neighbor index : 1
Chassis type   :MAC address
Chassis ID     :00e0-11fc-1710
Port ID type   :Interface name
Port ID        :GigabitEthernet0/0/1
Port description    :GigabitEthernet0/0/1
System name         :HUAWEI
System description  :S5735-S24T4X
Huawei Versatile Routing Platform Software
VRP (R) software,Version 5.160 (S5720 V200R023C00)
Copyright (C) 2000-2019 HUAWEI TECH CO., LTD
System capabilities supported   :bridge router
System capabilities enabled     :bridge router
Management address type  :ipv4
Management address value : 127.0.0.1
OID  :0.6.15.43.6.1.4.1.2011.5.25.41.1.2.1.1.1.
Expired time   :104s

Device 0 infomation:
  Device serial number :21980115830123456789
  Device model name    :S5735-S24T4X
Device 1 infomation:
  Device serial number :21980115790123456789
  Device model name    :S5735-S24T4X
Port VLAN ID(PVID)  :1
Port and protocol VLAN ID(PPVID)   :0
Port and protocol VLAN supported   :No
Port and protocol VLAN enabled     :No
VLAN name of VLAN  1: VLAN 0001
Protocol identity   :

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(1000)/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
Power type              :Type 2 PD
Power source            :PSE
Power priority          :Low
PD requested power value   :60.0(w)
PSE allocated power value  :60.0(w)
PD requested power mode A value  :30.0(w)
PD requested power mode B value  :30.0(w)
Power class             :6
Power typex             :Type 3 PSE
PSE allocated power mode A value :0.0(w)
PSE allocated power mode B value :0.0(w)
PSE maximum available power     :0.0(w)
PSE power pairsx        :Unknown
PSE Autoclass support       :PSE does not supports Autoclass
PD 4PID                 :PD does not supports powering of both Modes
PD Load                 :PD is single-signature or dual-signature and power demand on Mode A and
Mode B are not electrically isolated
Autoclass completed         :Autoclass idle
Autoclass request           :Autoclass idle
Power down              :Not power down
Power capability        :AF AT BT_60 BT_90
Power-up mode           :AT

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID     :0
Maximum frame Size      :9216

EEE support             :Yes
Transmit Tw             :16
Receive Tw              :16
Fallback Receive Tw     :65535
Echo Transmit Tw        :16
Echo Receive Tw         :16

MED Device information
Device class   :Network Connectivity

HardwareRev      :LE02MCUA VER.AVER.BVER.A
FirmwareRev      :151NA
SoftwareRev      :Version 5.160 V200R023C00
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:0.2(w)
```

Display information about neighbor devices of interfaces GigabitEthernet0/0/2. (The neighbor is an AP.)

```
<HUAWEI> display lldp neighbor interface gigabitethernet0/0/2
GigabitEthernet0/0/2 has 1 neighbor(s):
```



```
Neighbor index :1
Chassis type   :MAC address
Chassis ID     :00e0-11fc-8670
Port ID type   :Interface name
Port ID        :MultiGE0/0/1
Port description    :HUAWEI, AP Series, MultiGE0/0/1
Interface
System name         :e483-2696-8670
System description  :Huawei AP AirEngine8760-X1-PRO
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.170 (AirEngine8760-X1-PRO V200R022C10SPC100)
Copyright (C) 2011-2020 Huawei Technologies
Co.,Ltd

System capabilities supported   :wlanAccessPoint
System capabilities enabled     :wlanAccessPoint
Management address type  :ipv4
Management address value :169.254.1.1
OID  :0.6.15.43.6.1.4.1.2011.5.25.41.1.2.1.1.1.
Expired time   :105s

Device 0 infomation:
  Device serial number :
2102353GSG10LB000165
  Device model name    :AirEngine8760-X1-PRO

Port VLAN ID(PVID)  :1
VLAN name of VLAN  1:VLAN1

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(1000)/duplex(Full)

Power port class            :PD
PSE power supported         :No
PSE power enabled           :No
PSE pairs control ability   :No
Power pairs                 :Spare
Port power classification   :Class7
Power type                  :Type 2 PD
Power source                :PSE
Power priority              :Low
PD requested power value    :71.3(w)
PSE allocated power value   :71.3(w)
PD requested power mode A value  :35.6(w)
PD requested power mode B value  :35.6(w)
Power class                 :0
Power typex                 :Type 4 dual-signature PD
PSE allocated power mode A value :0.0(w)
PSE allocated power mode B value :0.0(w)
PSE maximum available power      :0.0(w)
PSE power pairsx            :Unknown
PSE power status            :Unknown
PD power status             :Powered single-signature PD
Dual-signature power class mode A:Single-signature PD or 2-pair only
PSE
Dual-signature power class mode B:Single-signature PD or 2-pair only
PSE
PSE Autoclass support       :PSE does not supports
Autoclass
PD 4PID                     :PD supports powering of both Modes
PD Load                     :PD is single-signature or dual-signature and power demand on Mode A and
Mode B are not electricall
y isolated
Autoclass completed         :Autoclass idle
Autoclass request           :Autoclass idle
Power down request          :YES
Power down timer            :1s
```



```
Power capability          :AT BT_60 BT_90
Power-up mode             :BT_90

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0

Maximum frame Size       :1800
```

Table 16-38 Description of the **display lldp neighbor** command output

Item	Description
Neighbor index	Index of a neighbor.
Chassis type	ID sub-types of a neighboring device: • Chassis component: chassis alias • Interface alias: interface alias • Port component: interface or backplane alias • MAC address: MAC address • Network address: network address • Interface name: name of the interface • Locally assigned: name of the local device
Chassis Id	ID of a neighboring device.
Port ID type	ID sub-type of a neighboring interface: • Interface alias: interface alias • Port component: interface or backplane alias • MAC address: MAC address • Network address: network address • Interface name: name of the interface • Agent circuit ID: circuit ID of the DHCP agent • Locally assigned: 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.

Item	Description
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
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	Neighbor management address type of a neighbor.
Management address value	Neighbor management address of a neighbor.
OID	Neighbor management address OID.
Expired time	Aging time of a neighbor.
Device 0 infomation Device 1 infomation	Neighbor device information. This field is displayed only when there are multiple neighbors.
Device serial number	Serial number of a neighbor.
Device model name	Model of a neighbor.
Port VLAN ID(PVID)	VLAN ID of an interface.
Port and protocol VLAN ID(PPVID)	Protocol VLAN ID of a port.

Item	Description
Port and protocol VLAN supported	Whether PPVID is supported: ● Yes: PPVID is supported. ● No: PPVID is not supported.
Port and protocol VLAN enabled	Whether PPVID is enabled: ● Yes: PPVID is enabled. ● No: PPVID is disabled.
VLAN name of VLAN 1	Name of VLAN 1.
Protocol identity	Protocol ID.
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.
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.

Item	Description
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. • Class5: indicates level 6. • Class6: indicates level 7. • Class7: indicates level 8. • Unknown: indicates an unknown control level.
Power type	The power supply type: • Type 1 PD: indicates the PD that does not support IEEE 802.3at. • Type 1 PSE: indicates the PSE that does not support IEEE 802.3at. • Type 2 PD: indicates the PD that supports IEEE 802.3at. • Type 2 PSE: indicates the PSE that supports IEEE 802.3at.
Power source	The power supply source.
Power priority	The power supply priority of an interface: • low • high • Critical • unknown
PD requested power value	Power requested by the PD.
PSE allocated power value	Power allocated by the PSE to the PD.
PD requested power mode A value	Power in alternative A mode requested by the PD.
PD requested power mode B value	Power in alternative B mode requested by the PD.
Power class	• When the power type is PD this field shall be set to the requested Class of the PD. • When the power type is PSE this field shall be set to the PSEs assigned Class.

Item	Description
Power typex	• Type 1 PSE • Type 1 PD • Type 2 PSE • Type 2 PD • Type 3 PSE • Type 3 single-signature PD • Type 4 PSE • Type 4 PD • Type 4 single-signature PD • Type 3 dual-signature PD • Type 4 dual-signature PD
PSE power status	• 2-pair powering • 4-pair powering single-signature PD • 4-pair powering dual-signature PD • Unknown
PD power status	• Powered single-signature PD • 2-pair powered dual-signature PD • 4-pair powered dual-signature PD • Unknown
Dual-signature power class mode A	• Class1 • Class2 • Class3 • Class4 • Class5 • Single-signature PD or 2-pair only PSE • Unknown
Dual-signature power class mode B	• Class1 • Class2 • Class3 • Class4 • Class5 • Single-signature PD or 2-pair only PSE • Unknown
PSE allocated power mode A value	Power allocated by the PSE to the PD in alternative A mode.
PSE allocated power mode B value	Power allocated by the PSE to the PD in alternative B mode.

Item	Description
PSE maximum available power	The highest power the PSE can grant to the PD.
PSE power pairsx	The power supply modes that the PSE supports: ● Alternative A ● Alternative B ● Alternative A and Alternative B ● Unknown
PSE Autoclass support	Whether PSE supports Autoclass: ● PSE supports Autoclass ● PSE does not support Autoclass
PD 4PID	● PD supports powering of both Modes ● PD does not support powering of both Modes
PD Load	● PD is dual-signature and power demand on Mode A and Mode B are electrically isolated ● PD is single-signature or dual-signature and power demand on Mode A and Mode B are not electrically isolated
Autoclass completed	Whether Autoclass is completed: ● Autoclass measurement completed ● Autoclass idle
Autoclass request	Whether the interface has received Autoclass request: ● PD requests Autoclass measurement ● Autoclass idle
Power down	Whether the interface powers down.
Power down request	Whether the interface sends a power-off request. ● YES ● NO
Power down timer	Time when the interface stops supplying power. This field is displayed only when **Power down request** is **YES**.
Power capability	Power supply mode supported by the PD: ● AF: 802.3af ● AT: 802.3at ● BT_60: 802.3bt with the 60 W supply power ● BT_90: 802.3bt with the 90 W supply power

Item	Description
Power-up mode	Power supply mode used by the PD. The setting -- indicates that the PD does not notify the switch of the power supply mode in use.
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.
EEE support	Whether the interface supports energy efficient Ethernet (EEE).
Transmit Tw	Amount of time the sender waits before starting sending data after leaving lower power consumption mode (LPI mode).
Receive Tw	Amount of time the receiver expects the sender to wait before starting sending data after leaving LPI mode.
Fallback Receive Tw	Additional information provided to the sender.
Echo Transmit Tw	Transmit Tw value specified in the Echo message sent from the remote end.
Echo Receive Tw	Receive Tw value specified in the Echo message sent from the remote end.
Device class	Type of the MED device.
HardwareRev	Hardware version of the device.
FirmwareRev	Firmware version of the device.
SoftwareRev	Software version of the device.
SerialNum	Serial number of the device. **NOTE** If the decimal value of a serial number is not in the range of 32 to 126, the serial number is displayed in octal notation.

Item	Description
Manufacturer name	Name of the manufacturer.
Model name	Name of a model.
Asset tracking identifier	Asset tracking ID.
Media policy type	Type of the media policy: ● Voice. ● Voice Signaling. ● Guest Voice. ● Guest Voice Signaling. ● Softphone Voice. ● Video Conferencing. ● Streaming Video. ● Video Signaling. ● 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 ● Unknown indicates that the Media policy VlanID, Media policy L2 priority and Media policy Dscp value fields are ignored.
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	802.1p priority.
Media policy Dscp	DSCP value.
Power Type	Power supply type: ● PSE: power-sourcing equipment. ● PD: powered device. ● Unknown: indicates an unknown power supply type.

Item	Description
PoE PSE power source	Type of the PSE: • Primary: indicates primary power supply. • Backup: indicates backup power supply. • Unknown: indicates an unknown type of PSE.
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

16.3.11 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 brief information about the LLDP neighbors of a switch and the interfaces connected to neighbors, run this command.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.

2. LLDP has been enabled on the interface using the **lldp enable** command.

Example

Display brief information about LLDP neighbors of the switch.

```
<HUAWEI> display lldp neighbor brief
Local Intf   Neighbor Dev          Neighbor Intf          Exptime(s)
GE0/0/1      Huawei                GE0/0/1                103
```

Table 16-39 Description of the **display lldp neighbor brief** command output

Item	Description
Local Intf	Local interface on which the LLDP neighbor relationship is established with a peer device.
Neighbor Dev	Name of an LLDP neighbor. If the name of an LLDP neighbor contains more than 24 characters, only the first 21 characters plus an ellipsis (...) are displayed. This display format cannot be changed. For example, if the name of an LLDP neighbor is **Huawei12345678912345678912345678 9**, this field is displayed **Huawei123456789123456...**. To view the complete neighbor name, run the **display lldp neighbor system-name** command.
Neighbor Intf	Interface of a peer device on which the LLDP neighbor relationship is established.
Exptime	Time left before an LLDP neighbor relationship expires, in seconds.

16.3.12 display lldp neighbor system-name

Function

The **display lldp neighbor system-name** command displays the name of an LLDP neighbor.

Format

display lldp neighbor system-name

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the name of an LLDP neighbor contains more than 24 characters, the **display lldp neighbor brief** command cannot display the complete name of the LLDP neighbor. In this case, run the **display lldp neighbor system-name** command instead.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Example

Display the name of an LLDP neighbor.

```
<HUAWEI> display lldp neighbor system-name
Local Interface  Neighbor Interface  Neighbor Device
GE0/0/3          GE0/0/1             Edge1i-11111111111111111111111111111111111111111111
```

Table 16-40 Description of the **display lldp neighbor system-name** command output

Item	Description
Local Interface	Local interface on which the LLDP neighbor relationship is established with a peer device.
Neighbor Interface	Interface of a peer device on which the LLDP neighbor relationship is established.
Neighbor Dev	Name of an LLDP neighbor. A maximum of 255 characters can be displayed in this field.

16.3.13 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

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

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

When you query statistics about all interfaces, no information about LLDP-disabled interfaces is displayed. When you query statistics about an LDDP-disabled interface, the system displays a message indicating that LLDP is not enabled on this interface.

Example

Display the statistics about LLDP packets sent and received by all interfaces.

```
<HUAWEI> display lldp statistics
LLDP statistics global Information:
```



```
Statistics for GigabitEthernet0/0/1:
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 16-41 Description of the **display lldp statistics** command output

Item	Description
LLDP statistics global Information	Statistics about LLDP packets.
Statistics for *x*	Statistics about LLDP packets received and sent by the *x* interface.
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.

16.3.14 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*]

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

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Example

Display Optional TLVs that can be sent with LLDP packets on GigabitEthernet0/0/1.

```
<HUAWEI> display lldp tlv-config interface gigabitethernet 0/0/1

LLDP tlv-config of port [GigabitEthernet0/0/1]:
-----------------------------------------------------
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
Protocol Identity TLV              No        No

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
EEE TLV                            Yes       Yes

LLDP-MED extend TLV:
-----------------------------------
Capabilities TLV                   Yes       Yes
Extended Power Via MDI TLV         Yes       Yes
Inventory TLV                      Yes       Yes
Network Policy TLV                 Yes       Yes
Location Identification TLV        No        No

LLDP Legacy config TLV:
-----------------------------------
Poe TLV                            Yes       Yes
Device Sn And Model TLV            Yes       Yes
Pnp TLV                            Yes       Yes
-----------------------------------
  Start Vlanid TLV                 Yes       Yes
  Link Aggregation TLV             Yes       Yes
  Device Type TLV                  Yes       Yes
```

Table 16-42 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.

Item	Description
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.
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.
EEE TLV	EEE capability TLV.
LLDP Legacy config TLV	Legacy TLV configuration.
Poe TLV	PoE power TLV.
Device Sn And Model TLV	Device SN and model TLV.
Pnp TLV	PnP TLV.
Start Vlanid TLV	Initial VLAN TLV.
Link Aggregation TLV	Link aggregation TLV.
Device Type TLV	Device type TLV.

16.3.15 ip domain-name

Function

The **ip domain-name** command adds a suffix to a device name.

The **undo ip domain-name** command deletes the suffix of a device name.

By default, a device name does not have a suffix.

NOTE

Only the SS1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, and S6720S-S support this command.

Format

ip domain-name *domain-name*

undo ip domain-name

Parameters

Parameter	Description	Value
domain-name	Specifies the suffix of a device name.	The value is a string of 1 to 255 characters without spaces. It contains digits, letters, hyphens (-), underscores (_), and dots (.).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device name and a suffix form a fully qualified domain name (FQDN). If you need to add a suffix to a device name, run the **ip domain-name** command. In this situation, the System Name TLV in an LLDP packet is in "device name.suffix" format. For example, if the device name is **HUAWEI** and suffix is **area1**, the System Name TLV in an LLDP packet is **HUAWEI.area1**.

Precautions

If you run this command multiple times, only the latest configuration takes effect.

Example

Set the device name suffix to **area1**.

```
<HUAWEI> system-view
[HUAWEI] ip domain-name area1
```

16.3.16 lldp auto-vlan sensor ap

Function

The **lldp auto-vlan sensor ap** command configures a switch to identify Huawei Fit APs using LLDP and adds the interfaces receiving the LLDP packets from APs to the specified VLAN.

The **undo lldp auto-vlan** command disables this function.

By default, this function is disabled.

Format

lldp auto-vlan *vlan-id* **sensor ap**

undo lldp auto-vlan *vlan-id* **sensor ap**

lldp auto-vlan tagged { *vlan-id1* [**to** *vlan-id2*] }&<1-10> **sensor ap**

undo lldp auto-vlan tagged { *vlan-id1* [**to** *vlan-id2*] }&<1-10> **sensor ap**

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN to which the interfaces receiving LLDP packets from APs are added in untagged mode.	The value is an integer that ranges from 1 to 4094.
tagged	Indicates that the interfaces receiving LLDP packets from APs are added to a VLAN in tagged mode.	-
vlan-id1 [**to** *vlan-id2*]	Specifies the VLAN to which the interfaces receiving LLDP packets from APs are added in tagged mode.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a switch is connected to a Huawei Fit AP, the interfaces connected to the AP must be added to the AP's management VLAN in untagged mode and to the AP's service VLAN in tagged mode. If many APs are connected to the switch, the configuration is complex. To facilitate operation, run the **lldp auto-vlan** *vlan-id* **sensor ap** command to enable the switch to automatically add the interfaces receiving LLDP packets from an AP to the AP's management VLAN in untagged mode, and run the **lldp auto-vlan tagged** { *vlan-id1* [**to** *vlan-id2*] }&<1-10> **sensor ap** command to add these interfaces to the AP's service VLAN in tagged mode.

You can run the **display port vlan** [*interface interface-number* | **active**] command to view information about the VLANs to which interfaces are automatically added.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command.

Precautions

- The ID of the VLAN to which interfaces are added in untagged mode cannot be the same as the ID of the VLAN to which the interfaces are added in tagged mode.
- The VLAN specified in the command can be an existing VLAN or created after this command is executed, but cannot be the control VLAN for SEP/RRPP/ERPS.
- After an interface is added in untagged mode to a specified VLAN, the original PVID of the interface becomes invalid. When the LLDP neighbor information of the interface ages (for example, the connected AP goes offline), the original PVID configuration takes effect again and the interface is automatically removed from the VLAN.
- If the VLAN to which an interface is added in tagged mode is the same as that manually configured on the interface, the manually configured VLAN takes effect.
- An interface can be automatically added to a VLAN in tagged mode only when the interface type is trunk or hybrid.

Example

Add the interfaces receiving LLDP packets from an AP to the management VLAN 100 in untagged mode and to the service VLAN 200 in tagged mode.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] lldp enable
[HUAWEI] lldp auto-vlan 100 sensor ap
[HUAWEI] lldp auto-vlan tagged 200 sensor ap
```


16.3.17 lldp clear neighbor

Function

The **lldp clear neighbor** command clears LLDP neighbors in the system or on an interface of the device.

Format

lldp clear neighbor [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Indicates the type and number of the interface whose LLDP neighbors to be cleared. In the command: • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If no interface is specified, this command clears LLDP neighbors on all interfaces.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want to obtain the latest LLDP neighbor information of interfaces, use the **lldp clear neighbor** command to clear existing LLDP neighbors. When an interface receives new LLDP packets, new LLDP neighbors are generated.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command.

Example

Clear LLDP neighbors of all interfaces.

```
<HUAWEI> lldp clear neighbor
Warning: This command will clear the neighbor information of all the ports. Continue? [Y/N]:y
```

16.3.18 lldp compliance cdp receive

Function

The **lldp compliance cdp receive** command enables CDP-compatible LLDP on an interface.

The **undo lldp compliance cdp receive** command disables CDP-compatible LLDP on an interface.

By default, CDP-compatible LLDP is disabled on an interface.

Format

lldp compliance cdp receive

undo lldp compliance cdp receive

Parameters

None

Views

MEth interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Neighbors may use other proprietary protocols but LLDP, for example, CDP. To ensure that the local device can discover and identify the neighbors, you can use this command to enable CDP-compatible LLDP on an interface.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

An Ethernet interface supports this command no matter whether it works in Layer 2 or Layer 3 mode.

Example

Enable CDP-compatible LLDP on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp compliance cdp receive
```

16.3.19 lldp compliance cdp txrx

Function

The **lldp compliance cdp txrx** command enables an interface to exchange information with CDP-capable devices.

The **undo lldp compliance cdp txrx** command disables an interface from exchanging information with CDP-capable devices.

By default, an interface cannot exchange information with CDP-capable devices.

Format

lldp compliance cdp txrx

undo lldp compliance cdp txrx

Parameters

None

Views

MEth interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some IP phones send proprietary protocol packets but not DHCP packets to apply for IP addresses. After you run the **lldp compliance cdp txrx** command on an interface, the switch can identify proprietary protocol packets sent from such the IP phone connected to the interface and respond to the proprietary protocol packets. In addition, the switch assigns the voice VLAN configured on the LLDP module to the IP phone.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

An Ethernet interface supports this command no matter whether it works in Layer 2 or Layer 3 mode.

When a switch connects the IP phones of some vendors, you are advised to run the **lldp tlv-enable med-tlv network-policy voice-vlan vlan** *vlan-id* command to specify the voice VLAN ID in the MED TLVs advertised from the interface.

Example

Enable GigabitEthernet0/0/1 to exchange information with CDP-capable voice devices.

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp tlv-enable med-tlv network-policy voice-vlan vlan 10
[HUAWEI-GigabitEthernet0/0/1] lldp compliance cdp txrx
```

16.3.20 lldp device-classifier enable

Function

The **lldp device-classifier enable** command enables the switch to automatically execute the Python script after the LLDP neighbor changes.

The **undo lldp device-classifier enable** command disables the switch from automatically executing the Python script after the LLDP neighbor changes.

By default, the switch is enabled to automatically execute the Python script after the LLDP neighbor changes.

Format

lldp device-classifier enable

undo lldp device-classifier enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a switch has multiple types of LLDP neighbors and needs to deliver different configurations to different types of LLDP neighbors, configure the Python script in

advance and run the **lldp device-classifier enable** command to enable the switch to automatically execute the Python script after the LLDP neighbor changes. If the switch detects that a specified type of LLDP neighbor is added or deleted on an interface, the switch automatically delivers the predefined configuration in the Python script, reducing the configuration workload.

Prerequisites

1. The Python script automatically executed after the LLDP neighbor changes has been prepared, uploaded, and installed, and the Python script assistant has been configured. For details, see "**Configuring OPS**" in OPS Configuration in *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Device Management*.
2. LLDP has been enabled globally using the **lldp enable (system view)** command.

Example

Enable the switch to automatically execute the Python script after the LLDP neighbor changes.

```
<HUAWEI> system-view
[HUAWEI] lldp device-classifier enable
```

16.3.21 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.

The **undo lldp dot3-tlv power** command restores the default configuration.

By default, the 802.3 Power Via MDI TLV conforms to 802.1ab.

Format

lldp dot3-tlv power { **802.1ab** [**force**] | **802.3at** }

undo lldp dot3-tlv power { **802.1ab force** | **802.3at** }

Parameters

Parameter	Description	Value
802.1ab	Indicates that the 802.3 Power Via MDI TLV sent by the interface conforms to 802.1ab.	-
802.3at	Indicates that the 802.3 Power Via MDI TLV sent by the interface conforms to 802.3at.	-

Parameter	Description	Value
force	Indicates that the 802.3 Power Via MDI TLV sent by the interface must conform to 802.1ab.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE 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:

- 802.1ab format: [TLV type | TLV information string length | 802.3 OUI | 802.3 subtype | MDI power support | PSE power pair | power class]
- 802.3at format: [TLV type | TLV information string length | 802.3 OUI | 802.3 subtype | MDI power support | PSE power pair | power class | type/source/priority | PD requested power value | PSE allocated power value]

Based on 802.1ab, 802.3at extends three fields: t**ype/source/priority**, **PD requested power value**, and **PSE allocated power value**.

If a PD requires higher power than the PoE switch can supply, run the **lldp dot3-tlv power 802.1ab force** command to specify that 802.3 Power Via MDI TLV sent by the interface must conform to 802.1ab, so as to reduce the power required by the PD.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

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. You are advised to retain the default configuration of the switch. That is, interfaces send 802.3 Power Via MDI TLV conforming to 802.1ab. The switch can then adapt to 802.3 Power Via MDI TLV conforming to 802.1ab or 802.3at based on the remote device and correctly communicates with the remote device.

An Ethernet interface supports the **lldp dot3-tlv power** command no matter whether it works in Layer 2 or Layer 3 mode.

An interface that is already configured with the **poe power auto-neg enable** command do not support the **lldp dot3-tlv power 802.1ab force** and **lldp dot3-tlv power 802.3at** commands.

Example

Configure the interface to send the 802.3 Power Via MDI TLV conforming to 802.3at.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp dot3-tlv power 802.3at
```

16.3.22 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

MEth interface view, Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

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

LLDP has been enabled globally using the **lldp enable (system view)** command.

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.

The **lldp enable (interface view)** command can be executed only on an Ethernet interface, regardless of whether it works at Layer 2 or Layer 3 mode, but not on a logical interface such as a VLANIF or Eth-Trunk interface. For an Eth-Trunk interface, LLDP can only be enabled on its member interfaces. LLDP-enabled interfaces and LLDP-disabled interfaces can exist in the same Eth-Trunk.

Example

Disable LLDP on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo lldp enable
```

16.3.23 lldp enable (system view)

Function

The **lldp enable** command enables LLDP globally.

The **undo lldp enable** command disables LLDP globally.

By default, LLDP is enabled 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

After the global LLDP is disabled, the LLDP configuration is deleted from all interfaces.

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.

For the device running a version earlier than V200R011C10SPC200:

- By default, LLDP is disabled globally, and the configuration file does not have the **undo lldp enable** configuration. After the device is upgraded to V200R011C10SPC200 or a later version, the configuration file has the **undo lldp enable** configuration.
- If **lldp enable** has been executed to enable LLDP globally, the configuration file has the **lldp enable** configuration. After the device is upgraded to V200R011C10SPC200 or a later version, the configuration file no longer has the **lldp enable** configuration.

The status of global LLDP does not change after the device is upgraded.

Example

Enable LLDP globally.

```
<HUAWEI> system-view
[HUAWEI] lldp enable
```

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
```


16.3.24 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.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command.

The management IP address to be allocated must be a valid unicast 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

If no management address is configured or an invalid management address is configured, the system sets an IP address in the address list as the management address. The system selects the IP address in the following sequence: IP address of the device connected to the iMaster NCE-Campus, loopback interface address, management port address, VLANIF interface address, VBDIF interface address, Layer 3 Ethernet interface address, and Sub-interface. Among the IP addresses of the same type, the system selects the smallest one. If the system fails to find a management IP address, the bridge MAC address is used as the management address.

Example

Set the LLDP management IP address to 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] lldp management-address 10.10.10.1
```

16.3.25 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 [*delay*]

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

LLDP has been enabled globally using the **lldp enable (system view)** command.

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.
- 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 seconds.

```
<HUAWEI> system-view
[HUAWEI] lldp message-transmission delay 5
```

16.3.26 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 [*hold*]

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.

After the LLDP function is disabled on the device, its neighbors wait until the TTL of the device information expires, and then delete the device information. This prevents network topology flapping.

Prerequisites

LLDP has been enabled globally using the **lldp enable (system view)** command.

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.

```
<HUAWEI> system-view
[HUAWEI] lldp message-transmission hold-multiplier 5
```

16.3.27 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 [*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

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

LLDP has been enabled globally using the **lldp enable (system view)** command.

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.

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.

```
<HUAWEI> system-view
[HUAWEI] lldp message-transmission interval 35
```

16.3.28 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 [*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

LLDP has been enabled globally using the **lldp enable (system view)** command.

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
```

16.3.29 lldp tlv-enable (MEth interface view)

Function

The **lldp tlv-enable** command sets the TLVs that can be sent by the MEth interface.

The **undo lldp tlv-enable** command sets the TLVs disabled on the MEth interface.

By default, the MEth interface can advertise all 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 med-tlv { **all** | **capability** | **inventory** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* } & <1-10> | **elin-address** *Tel-Number* } }

undo lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

undo lldp tlv-enable med-tlv { **all** | **capability** | **inventory** | **location-id** [**civic-address** | **elin-address**] }

Parameters

Parameter	Description	Value
all	Indicates to advertise all basic 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.	-
all	Indicates to advertise all MED TLVs except the Location Identification 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.	-

Parameter	Description	Value
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.	-
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.

Views

MEth 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. LLDPDUs supported by the management interface includes basic TLVs and MED TLVs.

Devices on both ends can have different TLV types configured. You only need to configure TLV types according to networking requirements.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

- If the **all** parameter is not specified, all the available TLVs of the specified type can be advertised except the 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.

Example

Configure The MEth interface to advertise the MED Capabilities TLV.

```
<HUAWEI> system-view
[HUAWEI] interface meth 0/0/1
[HUAWEI-MEth0/0/1] lldp tlv-enable med-tlv capability
```

16.3.30 lldp tlv-enable basic-tlv

Function

The **lldp tlv-enable basic-tlv** command sets the basic TLVs that can be sent by an interface.

The **undo lldp tlv-enable basic-tlv** command set the basic TLVs disabled on an interface.

By default, an interface can advertise all basic TLVs.

Format

lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

undo lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

Parameters

Parameter	Description	Value
all	Indicates to advertise all basic TLVs.	-
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.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group 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.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

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.

An Ethernet interface supports this command no matter whether it works in Layer 2 or Layer 3 mode.

Example

Configure GigabitEthernet0/0/1 to advertise all basic TLVs.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp tlv-enable basic-tlv all
```

16.3.31 lldp tlv-enable dot1-tlv

Function

The **lldp tlv-enable dot1-tlv** command sets to advertise TLVs defined by the IEEE 802.1 working group.

The **undo lldp tlv-enable dot1-tlv** command sets the TLVs defined by the IEEE 802.1 working group disabled on an interface.

By default, an interface advertises all TLVs defined by the IEEE 802.1 working group, except Protocol Identity TLV.

Format

lldp tlv-enable dot1-tlv { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [{ *vlan-id* [**to** *vlan-id1*] } &<1-14>] | **protocol-identity** }

undo lldp tlv-enable dot1-tlv { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [{ *vlan-id* [**to** *vlan-id1*] } &<1-14>] | **protocol-identity** }

Parameters

Parameter	Description	Value
all	Indicates to advertise all TLVs defined by the IEEE 802.1 working group.	-
port-vlan-id	Indicates to advertise Port VLAN ID TLV. The VLAN ID is the default VLAN ID on the interface.	-

Parameter	Description	Value
protocol-vlan-id [*vlan-id*]	Indicates to advertise Port And Protocol VLAN ID 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* [**to** *vlan-id1*] } &<1-14>]	Indicates to advertise VLAN Name TLV. If no VLAN ID is specified, the default VLAN ID is used. • *vlan-id* specifies the start VLAN ID. • **to** *vlan-id1* specifies the end VLAN ID. The value of *vlan-id1* must be greater than or equal to the value of *vlan-id1*.	The value of *vlan-id* is an integer that ranges from 1 to 4094. The value of *vlan-id1* is an integer that ranges from 1 to 4094.
protocol-identity	Indicates to advertise Protocol Identity TLV.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group 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.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

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.

NOTE

An Ethernet interface working in Layer 3 mode does not support the TLVs defined in IEEE 802.1.

Example

Configure GigabitEthernet0/0/1 to advertise the port VLAN TLV in the IEEE 802.1 format.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp tlv-enable dot1-tlv port-vlan-id
```

16.3.32 lldp tlv-enable dot3-tlv

Function

The **lldp tlv-enable dot3-tlv** command sets to advertise the TLVs defined by the IEEE 802.3 working group.

The **undo lldp tlv-enable dot3-tlv** command sets the TLVs defined by the IEEE 802.3 working group disabled on an interface.

By default, an interface advertises all TLVs defined by the IEEE 802.3 working group.

Format

lldp tlv-enable dot3-tlv { **all** | **eee** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** }

undo lldp tlv-enable dot3-tlv { **all** | **eee** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** }

Parameters

Parameter	Description	Value
all	Indicates to advertise all TLVs defined by the IEEE 802.3 working group.	-
eee	Indicates to advertise EEE (Energy Efficient Ethernet) TLV. EEE is supported only when the switch has only one neighbor.	-

Parameter	Description	Value
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.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group 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.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

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.

An Ethernet interface supports this command no matter whether it works in Layer 2 or Layer 3 mode.

Example

Configure GigabitEthernet0/0/1 to advertise the Link Aggregation TLV in the IEEE 802.3 format.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp tlv-enable dot3-tlv link-aggregation
```

16.3.33 lldp tlv-enable legacy-tlv esn

Function

The **lldp tlv-enable legacy-tlv esn** command enables the LLDPDUs sent by a device to carry ESN information.

The **undo lldp tlv-enable legacy-tlv esn** command disables the LLDPDUs sent by a device from carrying ESN information.

By default, the LLDPDUs sent by a switch carries ESN information.

Format

lldp tlv-enable legacy-tlv esn

undo lldp tlv-enable legacy-tlv esn

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Scenario

You can run the **undo lldp tlv-enable legacy-tlv esn** command to disable the LLDPDUs sent by a device from carrying ESN information.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command in the system view.
2. LLDP has been enabled on an interface using the **lldp enable** command in the interface view.

Example

Disable GE 0/0/2 from sending LLDPDUs carrying ESN information.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEIGigabitEthernet0/0/2] undo lldp tlv-enable legacy-tlv esn
```

16.3.34 lldp tlv-enable legacy-tlv poe

Function

The **lldp tlv-enable legacy-tlv poe** command enables the LLDPDUs sent by a device to carry the PoE power flag.

The **undo lldp tlv-enable legacy-tlv poe** command disables the LLDPDUs sent by a device from carrying the PoE power flag.

By default, the LLDPDUs sent by a switch carries the PoE power flag.

NOTE

This command is supported only on the following switch models:

S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5731-H, S5731-S, S5731S-S, S5732-H, S2730S-S, S5735-L1, S300, S5735-L, S5735-L-I, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735S-H, S5735S-S, S5735-S-I, S5736-S

Format

lldp tlv-enable legacy-tlv poe

undo lldp tlv-enable legacy-tlv poe

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Scenario

You can run the **undo lldp tlv-enable legacy-tlv poe** command to disable the LLDPDUs sent by a device from carrying the PoE power flag.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command in the system view.

2. LLDP has been enabled on an interface using the **lldp enable** command in the interface view.

Example

Disable GE 0/0/2 from sending LLDPDUs carrying the PoE power flag.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEIGigabitEthernet0/0/2] undo lldp tlv-enable legacy-tlv poe
```

16.3.35 lldp tlv-enable med-tlv

Function

The **lldp tlv-enable med-tlv** command sets to advertise the MED TLVs.

The **undo lldp tlv-enable med-tlv** command sets the MED TLVs disabled on an interface.

By default, an interface advertises all types of MED TLVs except the Location Identification TLV and Network Policy TLV.

NOTE

Although the interface does not advertise Network Policy TLV, Network Policy TLV is still enabled.

Format

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** [**voice-vlan** { **vlan** *vlan-id* [**cos** *cvalue* | **dscp** *dvalue*]* | **8021p** [**cos** *cvalue* | **dscp** *dvalue*]* | **untagged** }] | **power-over-ethernet** }

undo lldp tlv-enable med-tlv { **all** | **capability** | **inventory** | **location-id** [**civic-address** | **elin-address**] | **network-policy** [**voice-vlan** { **vlan** | **cos** | **dscp** | **8021p** | **untagged** }] | **power-over-ethernet** }

Parameters

Parameter	Description	Value
all	Indicates that all MED TLVs except Location Identification TLV and Network Policy TLV are advertised.	-
capability	Indicates to advertise MED Capabilities TLV.	-

Parameter	Description	Value
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.	-
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.

Parameter	Description	Value
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. **NOTE** An Ethernet interface working in Layer 3 mode does not support the Network Policy TLV.	-
voice-vlan	Encapsulates the voice VLAN ID when advertising Network Policy TLV.	-
vlan *vlan-id*	Specifies the voice VLAN ID.	The value is an integer that ranges from 1 to 4094.
cos *cvalue*	Specifies the CoS priority. The CoS priority is the PRI (Priority) field in an 802.1Q VLAN frame. This field is 3 bits long and ensures that high-priority data packets are forwarded first when congestion occurs.	The value is an integer that ranges from 0 to 7. The default value is 5. A larger value indicates a higher priority.
dscp *dvalue*	Sets the DSCP priority. The first six bits of the Type of Service (ToS) field in an IPv4 packet header are used as the DiffServ Code Point (DSCP). DSCP is used in the DiffServ model to provide QoS guarantee on an IP network. The operations performed by the traffic controller on the gateway are determined only by these six bits.	The value is an integer that ranges from 0 to 63. The default value is 46.
8021p	Sets the voice VLAN ID to VLAN 0.	-
untagged	Configures voice devices to send untagged voice data packets.	-

Parameter	Description	Value
power-over-ethernet	Advertises Extended Power via MDI TLV.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, port group 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.

Prerequisites

1. LLDP has been enabled globally using the **lldp enable** command.
2. LLDP has been enabled on the interface using the **lldp enable** command.

Precautions

- 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 802.3 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.
- When the switch detects that the LLDP packet sent by an LLDP neighbor on an interface contains any type of MED TLV, the switch advertises all MED TLVs that can be advertised on the interface to the LLDP neighbor. However, the LLDP neighbor may support only parts of MED TLVs advertised by the switch, leading to an LLDP negotiation failure. You can run the **undo lldp tlv-enable med-tlv** command to enable the interface not to advertise the MED TLV that is not supported by the LLDP neighbor. For example, if a terminal does not support the 802.3af standard, that is, Extended Power-via-MDI TLV cannot be identified, run the **undo lldp tlv-enable med-tlv power-over-ethernet** command on the interface connected to the terminal to enable the interface not to advertise Extended Power-via-MDI TLV.
- The voice VLAN configured using the **lldp tlv-enable med-tlv network-policy voice-vlan** command has a higher priority than the voice VLAN authorized by the authentication server.

Example

Configure GigabitEthernet0/0/1 to advertise the MED Capabilities TLV.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp tlv-enable med-tlv capability
```

16.3.36 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 [*interval*]

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

LLDP has been enabled globally using the **lldp enable (system view)** command.

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 delay takes effect for the lldpRemTablesChange trap generated when a neighbor is added, aged, or discarded (a new neighbor is discarded if the number of neighbors on an interface or switch has reached the upper limit).

Example

Set the delay in sending neighbor change traps to 6 seconds.

```
<HUAWEI> system-view
[HUAWEI] lldp trap-interval 6
```


16.3.37 reset cdp statistics

Function

The **reset cdp statistics** command clears statistics about CDP packets that all interfaces receive and send or CDP packets that a specified interface receives and sends.

Format

reset cdp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Interface on which statistics about CDP packets are to be cleared. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, CDP packet information about all interfaces is cleared.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want to quickly locate and process a CDP fault, you must calculate the numbers of CDP packets sent and received by a device for a specified period. Before collecting specific CDP packet statistics, you can run the **reset cdp statistics** command to clear existing statistics about CDP packets.

Prerequisites

LLDP has been globally enabled using the **lldp enable** command in the system view and LLDP has been configured to be compatible with CDP on interfaces using the **lldp compliance cdp receive** command.

Follow-up Procedure

After running the **reset cdp statistics** command to clear existing statistics about CDP packets, you can run the **display cdp statistics** command to check statistics about CDP packets sent and received by a device for a specific period.

Precautions

If you do not set the **interface** parameter when running the **reset cdp statistics** command, statistics about CDP packets sent and received by all interfaces are cleared. Exercise caution when running this command.

Example

Display statistics about CDP packets that all interfaces receive and send.

```
<HUAWEI> reset cdp statistics
```

16.3.38 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

LLDP has been enabled globally using the **lldp enable (system view)** command.

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 GigabitEthernet0/0/1.

```
<HUAWEI> reset lldp statistics interface gigabitethernet 0/0/1
```

16.4 Performance Management Commands

16.4.1 Command Support

Only the following switch models support Performance Management:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6720S-S, S6730-H, S6730S-H, S6730-S, S6730S-S

16.4.2 binding

Function

The **binding** command binds an instance to a performance statistics collection task.

The **undo binding** command unbinds an instance from a performance statistics collection task.

By default, no instance is bound to a performance statistics collection task.

Format

binding instance-type *instance-type* **all**

binding instance-type *instance-type* **instance** *instance-name* &<1-5>

undo binding instance-type *instance-type* { **all** | **instance** *instance-name* &<1-5> }

Parameters

Parameter	Description	Value
instance-type *instance-type*	Specifies the type of an instance bound to a performance statistics collection task.	The enumerated values include: • **ipfpm**: collects IP FPM statistics. • **uni-mng-as-port**: collects statistics on an AS port. • **wlan-ap**: collects AP statistics: • **wlan-radio**: collects statistics about a specified AP radio. • **wlan-ssid**: collects statistics about a service set bound to a specific AP radio. • **wlan-ap-wiredport**: collects statistics on an AP wired port. **NOTE** The S6720S-S only supports the **uni-mng-as-port**.
all	Binds all instances. When **all** is specified, *instance-type* can only be **ipfpm**.	-

Parameter	Description	Value
instance *instance-name*	Specifies the name of an instance of a specific type.	The value is a string of 1 to 255 case-insensitive characters. • When *instance-type* is **ipfpm**, the *instance-name* value is configured using the **instance (IPFPM-MCP view)** command. • When *instance-type* is **uni-mng-as-port**, the *instance-name* value is AS name +interface number, for example, as1 gigabitethernet0/0/1. • When *instance-type* is **wlan-ap**, the *instance-name* value is ap-id. For example, 1 indicates AP 1. • When *instance-type* is **wlan-radio**, the *instance-name* value is ap-id.radio-id. For example, 0.1 indicates radio 1 of AP 0. • When *instance-type* is **wlan-ssid**, the *instance-name* value is ap-id.radio-id.SSID name length.SSID name ASCII code. For example, 1.0.5.98.99.100.101.102 indicates the SSID with the name bcdef and name length 5 of radio 0 of AP 1. • When *instance-type* is **wlan-ap-wiredport**, the *instance-name* value is ap-id.port type x 100+port number. For example, 0.101 indicates FE port 1 of AP 0. The port type can be 1 (an FE port) or 2 (a GE port). The port number ranges from 0 to 99.

Views

Performance statistics collection task view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **binding** command is used to bind an instance to a performance statistics task so that the system can collect the performance statistics about the instance. Multiple instances can be bound to a performance statistics collection task.

Prerequisites

The traffic statistics function has been enabled using the **statistics enable** command. Otherwise, the **binding** command cannot take effect.

Precautions

If multiple performance statistics tasks are bound to the same interface to collect interface statistics, the peak values of the tasks are inaccurate.

If **instance-type** is set to **uni-mng-as-port**, performance statistics on interfaces of the AS are collected. The interval for collecting traffic statistics on interfaces configured by the **set flow-stat interval** *interval-time* command must be shorter than the interval for collecting performance statistics configured by the **statistics-cycle** *cycle* command. If the value of *interval-time* is greater than the value of *cycle*, performance statistics on interfaces are incorrect. This is because the statistics about the rate and bandwidth usage on interfaces remain the same within the interval specified by *interval-time*.

Example

Bind all instances in IP FPM to performance statistics collection task **task1**.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] quit
[HUAWEI-nqa-ipfpm-mcp] quit
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] binding instance-type ipfpm all
```

16.4.3 display pm brief

Function

The **display pm brief** command displays brief PM information.

Format

display pm brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After PM is configured, you can run the **display pm brief** command to view brief PM information, such as the PM status, number of performance statistics tasks, number of performance statistics files.

NOTE

Number of Active Statistics Objects in the output of the **display pm brief** command shows the number of current statistics objects. When this number exceeds 10000, you are advised to run the **statistics-cycle** command to set the statistics collection period to 30 minutes or longer, and run the s**ample-interval** command to set the sampling period to 5 minutes or longer.

Example

Display brief PM information.

```
<HUAWEI> display pm brief
Statistics Status                  : disable
Statistics Start Time              : -
Number of Statistics Tasks         : 2
Number of Active Statistics Objects : 0
Number of Configured Pm Servers    : 0
Number of Statistics Files         : 0
Statistics Files Saved Directory   : /pmdata/
```

Table 16-43 Description of the **display pm brief** command output

Item	Description
Statistics Status	Whether the performance statistics function is enabled: ● enable: enabled ● disable: disabled You can run the **statistics enable** command to configure this parameter.
Statistics Start Time	Time when the performance statistics function starts.
Number of Statistics Tasks	Number of performance statistics tasks.
Number of Active Statistics Objects	Number of current performance statistics objects.
Number of Configured Pm Servers	Number of configured PM servers.
Number of Statistics Files	Number of performance statistics files.
Statistics Files Saved Directory	Path where performance statistics files are saved.

16.4.4 display pm measure-info

Function

The **display pm measure-info** command displays information about performance statistics counters.

Format

display pm measure-info [**instance-type** *instance-type*]

Parameters

Parameter	Description	Value
instance-type *instance-type*	Specifies the type of an instance bound to a performance statistics task.	The enumerated values include: • **ipfpm**: collects IP FPM statistics. • **uni-mng-as-port**: collects statistics on an AS port. • **wlan-ap**: collects AP statistics: • **wlan-radio**: collects statistics about a specified AP radio. • **wlan-ssid**: collects statistics about a service set bound to a specific AP radio. • **wlan-ap-wiredport**: collects statistics on an AP wired port. **NOTE** The S6720S-S only supports the **uni-mng-as-port**.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running the **measure disable** command to configure performance statistics counters for instances of a specific type, run the **display pm measure-info** command to view information about available performance statistics counters, including the name, type, maximum value, and minimum value of each counter.

Example

Display information about performance statistics counters of the instance of the IPFPM type.


```
<HUAWEI> display pm measure-info instance-type ipfpm
Total instance types: 1, total measures: 10
------------------------------------------------------------------------------
Instance Type: ipfpm, Measures Count: 10
  Measure Name                : forward-loss-ratio-max
  Measure Type                : Maximum
  Measure Counter Size(bits)  : 32
  Measure MaxValue            : 100000000
  Measure MinValue            : -100000000

  Measure Name                : forward-loss-ratio-min
  Measure Type                : Minimum
  Measure Counter Size(bits)  : 32
  Measure MaxValue            : 100000000
  Measure MinValue            : -100000000

  Measure Name                : forward-loss-pkts-inc
  Measure Type                : Increase
  Measure Counter Size(bits)  : 64
  Measure MaxValue            : 9223372036854775807
  Measure MinValue            : -9223372036854775808
......
```

Table 16-44 Description of the **display pm measure-info** command output

Item	Description
Total instance types	Total types of measurement instances.
total measures	Total statistics counters.
Instance Type	Type of an instance.
Measures Count	Number of a performance statistics counter.
Measure Name	Name of a performance statistics counter.
Measure Type	Type of a performance statistics counter. The value can be: • Increase: Accumulated performance statistics are compared with the counter. • Actual: The currently collected performance statistics are compared with the counter. • Maximum: The maximum performance statistics are compared with the counter. • Minimum: The minimum performance statistics are compared with the counter. • Average: The average performance statistics are compared with the counter.
Measure Counter Size(bits)	Size of a performance statistics counter, 32 bits or 64 bits.
Measure MaxValue	Maximum value of a performance statistics counter.
Measure MinValue	Minimum value of a performance statistics counter.

16.4.5 display pm statistics

Function

The **display pm statistics** command displays the collected performance statistics.

Format

display pm statistics *task-name* **data-index** *index* [**instance-type** *instance-type* [**measure** *measure-name* | **instance** *instance-name* &<1-5>] *]

Parameters

Parameter	Description	Value
task-name	Displays the performance statistics of a specified performance statistics collection task.	The value is a string of 1 to 31 case-insensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.
data-index *index*	Displays the performance statistics collected at a specified interval.	The value is an integer that ranges from 0 to 16. ● If the value is 0, the current performance statistics are displayed. ● If the value is larger than 0, the performance statistics collected in one or more cycles are displayed. The smaller the value, the latest the statistics. If a short performance statistics collection cycle (5, 10, 15, 30, or 60 minutes) is set, the value of *index* ranges from 1 to 16. If a long performance statistics collection cycle (1440 minutes) is set, the value of *index* ranges from 1 to 3.

Parameter	Description	Value
instance-type *instance-type*	Specifies the type of an instance bound to a performance statistics collection task.	The enumerated values include: • **ipfpm**: collects IP FPM statistics. • **uni-mng-as-port**: collects statistics on an AS port. • **wlan-ap**: collects AP statistics: • **wlan-radio**: collects statistics about a specified AP radio. • **wlan-ssid**: collects statistics about a service set bound to a specific AP radio. • **wlan-ap-wiredport**: collects statistics on an AP wired port. **NOTE** The S6720S-S only supports the **uni-mng-as-port**.
measure *measure-name*	Specifies the name of a statistics counter.	The value is a string of 1 to 63 case-insensitive characters without spaces. Select statistics counters according to the device configuration.
instance *instance-name*	Specifies the name of an instance.	The value is a string of 1 to 255 case-insensitive characters. • When *instance-type* is **ipfpm**, the *instance-name* value is configured using the **instance (IPFPM-MCP view)** command. • When *instance-type* is **uni-mng-as-port**, the *instance-name* value is AS name+interface number, for example, as1 gigabitethernet0/0/1. • When *instance-type* is **wlan-ap**, the *instance-name* value is ap-id. For example, 1 indicates AP 1. • When *instance-type* is **wlan-radio**, the *instance-name* value is ap-id.radio-id. For example, 0.1 indicates radio 1 of AP 0. • When *instance-type* is **wlan-ssid**, the *instance-name* value is ap-id.radio-id.SSID name length.SSID name ASCII code. For example, 1.0.5.98.99.100.101.102 indicates the SSID with the name bcdef and name length 5 of radio 0 of AP 1. • When *instance-type* is **wlan-ap-wiredport**, the *instance-name* value is ap-id.port type x 100+port number. For example, 0.101 indicates FE port 1 of AP 0. The port type can be 1 (an FE port) or 2 (a GE port). The port number ranges from 0 to 99.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To view the current or historical performance statistics, run the **display pm statistics** command. The system can display the current performance statistics and historical performance statistics collected in a maximum of 16 cycles.

Prerequisites

- An instance has been bound to the current performance statistics using **binding** command.
- Performance statistics has been enabled for the current performance statistics task using **statistics enable** command.

Precautions

To display the performance statistics, confirm that the performance statistics task is running.

Example

Display the current performance statistics of the performance statistics collection task **task1**.

```
<HUAWEI> display pm statistics task1 data-index 0
Total measures count: 10
------------------------------------------------------------------------------
Instance Type        : ipfpm
Instance Name        : 1
Measure Name         : forward-loss-ratio-max
Measure Data         : 0
Valid Flag           : no statistics
Timestamp            : 2014-04-15 11:17:00

......
```

Table 16-45 Description of the **display pm statistics** command output

Item	Description
Total measures count	Number of a performance statistics counter.
Instance Type	Type of an instance bound to a performance statistics collection task.
Instance Name	Name of an instance bound to a performance statistics collection task.

Item	Description
Measure Name	Name of a performance statistics counter.
Measure Data	Statistics counter.
Valid Flag	Valid flag of the performance statistics. The value can be: • no statistics: The performance statistics are not collected. • valid: The performance statistics are valid. • incredible value: The performance statistics are not reliable. • measure not configured: The statistics counter is disabled.
Timestamp	Time when the performance statistics are collected.

16.4.6 display pm statistics-file

Function

The **display pm statistics-file** command displays performance statistics files.

Format

display pm statistics-file [*task-name*]

Parameters

Parameter	Description	Value
task-name	Displays the performance statistics files generated for a performance statistics task.	The value is a string of 1 to 31 case-insensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a performance statistics task starts, the system automatically generates performance statistics files for the task. To view the performance statistics files generated for the performance statistics task, run the **display pm statistics-file** command.

Example

Display performance statistics files for all performance statistics tasks.

```
<HUAWEI> display pm statistics-file
Total files count: 1
------------------------------------------------------------------------------
Task Name: test
  test20130701150001.txt
```

Table 16-46 Description of the **display pm statistics-file** command output

Item	Description
Total files count	Number of performance statistics files.
Task Name	Name of a performance statistics task. You can run the **statistics-task** command to configure this parameter.
test20130701150001.txt	Name of the performance statistics file.

16.4.7 display pm statistics-task

Function

The **display pm statistics-task** command displays information about a performance statistics collection task.

Format

display pm statistics-task [*task-name*]

Parameters

Parameter	Description	Value
task-name	Displays the information about a specified performance statistics collection task.	The performance statistics collection task must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check information about a performance statistics collection task, including the running status of the task, statistics collection cycle, and type of the instance bound to the task.

Example

Display information about performance statistics collection tasks.

```
<HUAWEI> display pm statistics-task
Total task count: 1
------------------------------------------------------------------------------
Task Name               : task1
Task State              : ready
Record-file Status      : enable
Threshold Alarm Status  : disable
Task Cycle              : 15 minutes
Sample Interval         : 3 minutes
Instance Type           : -
Record Interval(cycle)  : 4
File Format             : text
File Name Prefix        : task1
File Transfer Mode      : passive
Current File Name       : -
```

Table 16-47 Description of the **display pm statistics-task** command output

Item	Description
Total task count	Number of performance statistics collection tasks.
Task Name	Name of a performance statistics collection task. The task name is specified in the **statistics-task** *task-name* command.
Task State	Running status of a performance statistics collection task.
Record-file Status	Whether performance statistics file generation is enabled. The value can be: ● enable: This function is enabled. ● disable: This function is not enabled. This function is configured using the **record-file disable** command.
Threshold Alarm Status	Whether the threshold alarm function is enabled. The value can be: ● enable: This function is enabled. ● disable: This function is not enabled. This function is configured using the **threshold-alarm enable** command.
Task Cycle	Performance statistics collection cycle configured in a performance statistics collection task. This parameter is configured using the **statistics-cycle** *cycle* command.

Item	Description
Sample Interval	Sampling interval configured in a performance statistics collection task. This parameter is configured using the **sample-interval** *interval* command.
Instance Type	Type of an instance bound to a performance statistics collection task. This parameter is configured using the **binding instance-type** *instance-type* { **all** | **instance** *instance-name* &<1-5> } command.
Record Interval(cycle)	Interval at which the system generates performance statistics files. This parameter is configured using the **record-interval** *interval* command.
File Format	Format of performance statistics files.
File Name Prefix	Name prefix of a performance statistics file.
File Transfer Mode	Mode in which statistics files are uploaded to the performance management server. The value can be: • active: The device automatically uploads statistics files to the performance management server, this function is configured using the **upload auto** command. • passive: The device uploads statistics files to the performance management server following the instructions from the command line interface or network management system, this function is configured using the **upload** command.
Current File Name	Name of the current performance statistics file.

16.4.8 measure disable

Function

The **measure disable** command disables statistics counters in a performance statistics task.

The **undo measure disable** or **measure enable** command enables statistics counters in a performance statistics task.

By default, all statistics counters of the instance bound to the performance statistics collection task are measured.

Format

measure disable [*measure-name*]

undo measure disable [*measure-name*]

measure enable [*measure-name*]

Parameters

Parameter	Description	Value
measure-name	Specifies the name of a statistics counter in a performance statistics collection task.	The value is a string of 1 to 63 case-insensitive characters without spaces. Select statistics counters according to the device configuration.

Views

Performance statistics collection task view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the type of the instance bound to a performance statistics task is specified, statistics counters of instances of the specified type are enabled by default. The **measure disable** command can be used to disable some or all statistics counters.

After you run the **measure disable** [*measure-name*] command, some or all statistics counters are disabled. To add one or more counters that have been disabled to the performance statistics task again, run the **measure enable** [*measure-name*] or **undo measure disable** [*measure-name*] command to enable these counters.

Prerequisites

An instance has been bound to a performance statistics task using the **binding instance-type** *instance-type-name* **instance** *instance-name* command.

The performance statistics function has been enabled using the **statistics enable** command.

Example

Disable measurement of the forward-loss-ratio-max counter for ipfpm instances.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] binding instance-type ipfpm all
[HUAWEI-pm-statistics-task1] measure disable forward-loss-ratio-max
```


16.4.9 path

Function

The **path** command configures the destination path to save performance statistics files on the PM server.

The **undo path** command deletes the configured destination path.

By default, performance statistics files are uploaded to the default path on a PM server.

Format

path *destination-path*

undo path

Parameters

Parameter	Description	Value
destination-path	Specifies the destination path to save performance statistics files on the PM server.	The value is a string of 1 to 63 case-sensitive characters without spaces.

Views

PM server view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To upload performance statistics files to a specific path on the PM server, run the **path** command to specify the destination path.

Precautions

The specified destination path must exist in the performance management server. Otherwise, the statistics file cannot be uploaded to the server.

Example

Specify the destination path to save performance statistics on the PM server.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] pm-server server1
[HUAWEI-pm-server-server1] path d:/pmdata
```


16.4.10 pm

Function

The **pm** command displays the PM view.

Format

pm

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable the performance statistics function of PM, run the **pm** command to display the PM view.

Example

Display the PM view.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm]
```

16.4.11 pm-server

Function

The **pm-server** command creates a process serving the PM server and displays the view of the PM server created in the process. If there is an existing PM server view, the **pm-server** command displays the PM server view without creating a process.

The **undo pm-server** command deletes the created process.

By default, no process serving the PM server is created.

Format

pm-server *server-name*

undo pm-server *server-name*

Parameters

Parameter	Description	Value
server-name	Specifies the name of the process serving the PM server.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.

Views

PM view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To upload generated performance statistics files to the PM server, run the **pm-server** command to create a process serving the PM server.

Follow-up Procedure

Configure the IP address and port number for the PM server, and user name and password for logging in to the PM server. Performance statistics files are uploaded to the PM server using FTP or SFTP.

Precautions

If a device is enabled to upload performance statistics files to a PM server, the process serving the PM server cannot be deleted.

Example

Create a process named **server1** to serve the PM server.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] pm-server server1
[HUAWEI-pm-server-server1]
```

16.4.12 protocol (PM server view)

Function

The **protocol** command configures the parameters for connecting to a PM server.

The **undo protocol** command deletes the parameters for connecting to a PM server.

By default, no PM server connection parameter is configured.

Format

protocol { **ftp** | **sftp** } **ip-address** *ip-address* [**port** *port-number* | { **net-manager-vpn** | **vpn-instance** *vpn-instance-name* }] *

undo protocol

Parameters

Parameter	Description	Value
ftp	Uses the FTP protocol to upload performance statistics files.	-
sftp	Uses the SFTP protocol to upload performance statistics files.	-
ip-address *ip-address*	Specifies the IP address of the PM server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number.	The value is an integer that ranges from 1 to 65535. The default port number is 21 (using FTP) or 22 (using SFTP).
net-manager-vpn	Indicates the network management VPN.	-
vpn-instance *vpn-instance-name*	Specifies a VPN instance name.	The value must be an existing VPN instance name.

Views

PM server view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To upload statistics files to a PM server, use this command to configure connection parameters, including the transfer protocol, IP address, and port number of the PM server.

If the PM server uses a private IP address, you can use the **net-manager-vpn** parameter to specify a network management VPN or use the **vpn-instance** *vpn-instance-name* parameter to specify a VPN instance to upload a performance statistics file.

Precautions

Using FTP to upload performance statistics files is insecure. Therefore, using SFTP is recommended.

Example

Configure the device to upload performance statistics files to the SFTP server with the IP address 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] pm-server server1
[HUAWEI-pm-server-server1] protocol sftp ip-address 10.1.1.1
```

16.4.13 record-file disable

Function

The **record-file disable** command disables performance statistics file generation.

The **undo record-file disable** command restores performance statistics file generation.

By default, a performance statistics file is automatically generated and saved on the device. A maximum of four performance statistics files can be generated for each performance statistics collection task.

Format

record-file disable

undo record-file disable

Parameters

None

Views

Performance statistics collection task view

Default Level

2: Configuration level

Usage Guidelines

To save system resources, reduce system cost and operations on storage devices, and prolong the lifespan of storage devices during performance statistics collection, run the **record-file disable** command to prevent performance statistics files from being generated.

The system-generated file name is named in the format of "name of a performance statistics task+time that a performance statistics file is generated", and is saved in the text format. Each performance statistics collection task can

generate a maximum of four statistics files. If more than four statistics files are generated, the new file replaces the earliest one.

Example

Disable performance statistics file generation.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] record-file disable
```

16.4.14 record-interval

Function

The **record-interval** command sets the number of performance statistics collection cycles after which the system generates a statistics file.

The **undo record-interval** command restores the default number of performance statistics collection cycles.

By default:

- If a short performance statistics collection cycle (5, 10, 15, 30, or 60 minutes) is set, the system generates a statistics file after four cycles.
- If a long performance statistics collection cycle (1440 minutes) is set, the system generates a statistics file after one cycle.

Format

record-interval *interval*

undo record-interval

Parameters

Parameter	Description	Value
interval	Specifies the number of performance statistics collection cycles.	The value is an integer. The value range depends on the performance statistics collection cycle: • If a short performance statistics collection cycle is set, the value of *interval* ranges from 1 to 16, and the default value is 4. • If a long performance statistics collection cycle is set, the value of *interval* ranges from 1 to 3, and the default value is 1.

Views

Performance statistics collection task view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you configure a performance statistics collection task, the system periodically saves collected performance data to statistics files. To set the interval at which the system generates statistics files, run the **record-interval** command. Then the system generates performance statistics files every *cycle* x *interval* minutes, and automatically saves the performance data in the files. The system generates a maximum of four statistics files for each performance statistics collection task, and saves performance statistics files to the path flash: /pmdata by default.

Prerequisites

1. The performance statistics function has been enabled using the **statistics enable** command.
2. The *cycle* has been set using the **statistics-cycle** command.

Example

Configure the system to save performance data to a statistics file every three performance statistics collection cycles. If the performance statistics collection cycle is 5 minutes, the system saves a performance data to a statistics file every 15 minutes.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics enable
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] statistics-cycle 5
Warning: All data of the statistics task will be deleted. Continue? [Y/N]: y
[HUAWEI-pm-statistics-task1] record-interval 3
Warning: This operation will cause some data to be lost. Continue? [Y/N]: y
```

16.4.15 reset pm current-data

Function

The **reset pm current-data** command deletes the collected performance statistics.

Format

reset pm current-data [**instance-type** *instance-type* [**measure** *measure-name* | **instance** *instance-name* &<1-5>] *]

Parameters

Parameter	Description	Value
instance-type *instance-type*	Deletes the performance statistics about instances of a specified type. If **instance-type** *instance-type* is not specified, the system deletes the performance statistics about instances of all types.	The enumerated values include: • **ipfpm**: collects IP FPM statistics. • **uni-mng-as-port**: collects statistics on an AS port. • **wlan-ap**: collects AP statistics: • **wlan-radio**: collects statistics about a specified AP radio. • **wlan-ssid**: collects statistics about a service set bound to a specific AP radio. • **wlan-ap-wiredport**: collects statistics on an AP wired port. **NOTE** The S6720S-S only supports the **uni-mng-as-port**.
measure *measure-name*	Deletes the performance statistics about a specified counter.	The value is a string of 1 to 63 case-insensitive characters without spaces. Select statistics counters according to the device configuration.

Parameter	Description	Value
instance *instance-name*	Deletes the performance statistics about a specified instance.	The value is a string of 1 to 255 case-insensitive characters. • When *instance-type* is **ipfpm**, the *instance-name* value is configured using the **instance (IPFPM-MCP view)** command. • When *instance-type* is **uni-mng-as-port**, the *instance-name* value is AS name +interface number, for example, as1 gigabitethernet0/0/1. • When *instance-type* is **wlan-ap**, the *instance-name* value is ap-id. For example, 1 indicates AP 1. • When *instance-type* is **wlan-radio**, the *instance-name* value is ap-id.radio-id. For example, 0.1 indicates radio 1 of AP 0. • When *instance-type* is **wlan-ssid**, the *instance-name* value is ap-id.radio-id.SSID name length.SSID name ASCII code. For example, 1.0.5.98.99.100.101.102 indicates the SSID with the name bcdef and name length 5 of radio 0 of AP 1. • When *instance-type* is **wlan-ap-wiredport**, the *instance-name* value is ap-id.port type x 100+port number. For example, 0.101 indicates FE port 1 of AP 0. The port type can be 1 (an FE port) or 2 (a GE port). The port number ranges from 0 to 99.

Views

Performance statistics collection task view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To delete the collected performance statistics and collect new performance statistics, run the **reset pm current-data** command.

Precautions

Performance statistics cannot be restored after being deleted. Confirm your action before using this command.

Example

Delete the collected performance statistics.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] reset pm current-data
```

16.4.16 retry

Function

The **retry** command sets the number of retransmissions for a performance statistics file.

The **undo retry** command restores the number of retransmissions for a performance statistics file to the default value.

The default number of retransmissions for a performance statistics file is 3.

Format

retry *retry-times*

undo retry

Parameters

Parameter	Description	Value
retry-times	Sets the number of retransmissions for a performance statistics file.	The value is an integer ranging from 1 to 3. The default value is 3.

Views

PM server view

Default Level

2: Configuration level

Usage Guidelines

The system generates performance statistics files and transmits these files to a PM server. To set the number of retransmissions for a performance statistics file, run the **retry** command.

Example

Set the number of retransmissions for a performance statistics file to 2.

```
<HUAWEI> system-view
[HUAWEI] pm
```



```
[HUAWEI-pm] pm-server server1
[HUAWEI-pm-server-server1] retry 2
```

16.4.17 sample-interval

Function

The **sample-interval** command configures the sampling interval for a performance statistics task.

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

By default, the sampling interval varies with the performance statistics interval as follows:

- If the interval at which the performance statistics are collected is 5 minutes, the default sampling interval is 1 minute.
- If the interval at which the performance statistics are collected is 10 minutes, the default sampling interval is 2 minutes.
- If the interval at which the performance statistics are collected is 15 minutes, the default sampling interval is 3 minutes.
- If the interval at which the performance statistics are collected is 30 minutes, the default sampling interval is 5 minutes.
- If the interval at which the performance statistics are collected is 60 minutes, the default sampling interval is 5 minutes.
- If the interval at which the performance statistics are collected is 1440 minutes, the default sampling interval is 15 minutes.

Format

sample-interval *interval*

undo sample-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which the performance statistics collected in a performance statistics task is sampled.	The value can be 1, 2, 3, 5, 10, 15, 30, or 60, in minutes: • If the interval at which performance statistics are collected is 5 minutes, the sampling interval is 1 minute by default and can be set to 1 minute or 5 minutes. • If the interval at which performance statistics are collected is 10 minutes, the sampling interval is 2 minutes by default and can be set to 1, 2, 5, or 10 minutes. • If the interval at which performance statistics are collected is 15 minutes, the sampling interval is 3 minutes by default and can be set to 1, 3, 5, or 15 minutes. • If the interval at which performance statistics are collected is 30 minutes, the sampling interval is 5 minutes by default and can be set to 1, 2, 3, 5, 10, 15, or 30 minutes. • If the interval at which performance statistics are collected is 60 minutes, the sampling interval is 5 minutes by default and can be set to 1, 2, 3, 5, 10, 15, 30, or 60 minutes. • If the interval at which performance statistics are collected is 1440 minutes, the sampling interval is 15 minutes by default and can be set to 1, 2, 3, 5, 10, 15, 30, or 60 minutes.

Views

Performance statistics task view

Default Level

2: Configuration level

Usage Guidelines

After the statistics task is configured, the system collects statistics at a specified sampling interval. The shorter the sampling interval, the more accurate the statistics. However, more system resources are consumed.

Example

Set the sampling interval to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] pm
```



```
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] sample-interval 5
```

16.4.18 statistics enable

Function

The **statistics enable** command enables the performance statistics function.

The **undo statistics enable** command disables the performance statistics function.

By default, the performance statistics function is disabled.

Format

statistics enable

undo statistics enable

Parameters

None

Views

PM view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect performance statistics, run the **statistics enable** command to enable the performance statistics function.

Precautions

After the **undo statistics enable** command is run, the performance statistics task that is running will be stopped. Therefore, exercise caution when you run this command.

Example

Enable the performance statistics function.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics enable
```


16.4.19 statistics-cycle

Function

The **statistics-cycle** command configures the performance statistics collection interval for a performance statistics task.

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

The default interval is 15 minutes.

Format

statistics-cycle *cycle*

undo statistics-cycle

Parameters

Parameter	Description	Value
cycle	Specifies the performance statistics collection interval for a performance statistics task.	The value can be 5, 10, 15, 30, 60, or 1440, in minutes. The default value is 15 minutes. The system defines the interval 1440 minutes as a long interval and the interval 5, 10, 15, 30, or 60 minutes as a short interval.

Views

Performance statistics task view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A specific performance statistics collection interval is set for each performance statistics task. After the performance statistics collection interval is set, bind an instance to the performance statistics task and enable statistics counter measurement so that the system can collect performance statistics at the specified interval. If the statistics interval is set to a small value, the obtained performance statistics are more accurate but more system resources are consumed.

Configuration Impact

Running the **statistics-cycle** command in the performance statistics task view has the following impacts:

- Performance statistics of the performance statistics task are deleted.

- The default interval at which the system generates performance statistics files is used. In the case of a short statistics collection interval, the system generates a performance statistics file every four performance statistics collection intervals; in the case of a long statistics collection interval, the system generates a performance statistics file every one performance statistics collection interval.

Prerequisites

The performance statistics function has been enabled using the **statistics enable** command.

Example

Set the performance statistics collection interval for the performance statistics task named **task1** to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] statistics-cycle 5
Warning: All data of the statistics task will be deleted. Continue? [Y/N]: y
```

16.4.20 statistics-task

Function

The **statistics-task** command creates a performance statistics task or displays the performance statistics task view.

The **undo statistics-task** command deletes a performance statistics task.

By default, no performance statistics task is created.

Format

statistics-task *task-name*

undo statistics-task *task-name*

Parameters

Parameter	Description	Value
task-name	Specifies the name of a performance statistics task.	The value is a string of 1 to 31 case-insensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.

Views

PM view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A performance statistics task is the minimum statistics collection unit of PM. Before configuring the performance statistics function, run the **statistics-task** command to create a performance statistics task. Only one performance statistics collection interval can be configured for each performance statistics task. After a performance statistics task is configured, enable statistics counter measurement for the task.

Precautions

- A maximum of 16 performance statistics tasks can be configured.
- After the **undo statistics-task** command is run to delete a performance statistics task, performance statistics and performance statistics files of the task are deleted.

Prerequisites

The performance statistics function has been enabled using the **statistics enable** command.

Example

Configure a performance statistics task named **task1**.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1]
```

16.4.21 threshold-alarm enable

Function

The **threshold-alarm enable** command enables the threshold alarm.

The **undo threshold-alarm enable** command disables the threshold alarm.

By default, the threshold alarm function is disabled.

Format

threshold-alarm enable

undo threshold-alarm enable

Parameters

None

Views

Performance statistics task view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The threshold alarm function enables users to learn the device operating status in a timely manner so that the device maintenance level can be promoted. To monitor the running data, run the command to enable the threshold alarm.

Precautions

After the **undo threshold-alarm enable** command is run, the threshold alarm function will be disabled and threshold alarms will be cleared. Exercise caution before operation.

Follow-up Procedure

After the command is run, run the **threshold-alarm measure** command to configure monitoring rules for the threshold alarm. Otherwise, the threshold alarm function will not take effect.

Example

Enable the threshold alarm function.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] threshold-alarm enable
```

16.4.22 threshold-alarm measure

Function

The **threshold-alarm measure** command creates monitoring rules for threshold alarms.

The **undo threshold-alarm measure** command deletes monitoring rules for threshold alarms.

By default, no monitoring rules are created for threshold alarms about performance statistics tasks.

Format

threshold-alarm measure *measure-name* **operation** { **ge** | **le** } **trigger-value** *trigger-value-val* **clear-value** *clear-value-val*

undo threshold-alarm measure *measure-name* **operation** { **ge** | **le** }

Parameters

Parameter	Description	Value
measure-name	Specifies the threshold monitoring indicator The indicator name is predefined by each feature.	The value is a string of 1 to 63 case-insensitive characters without spaces. Select statistics counters according to the device configuration.
operation { **ge** | **le** }	Specifies the type of triggering a threshold alarm.	Enumerated value: ge or le • ge: the system triggers an alarm if the monitored indicator value is greater than or equal to the threshold value • le: the system triggers an alarm if the monitored indicator value is less than or equal to the threshold value.
trigger-value *trigger-value-val*	Specifies the threshold information when the alarm is triggered.	The value is an integer, and the value range is determined by *measure-name*.
clear-value *clear-value-val*	Specifies the threshold information when the alarm is cleared.	The value is an integer, and the value range is determined by *measure-name*.

Views

Performance statistics task view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The threshold alarm function is used for the system to periodically monitor the device operating status. If an alarm condition is triggered, the alarm will be sent to the NMS and cleared after the alarm condition is cleared.

The **threshold-alarm measure** command configures threshold monitoring rules for current performance statistics tasks. The **threshold-alarm measure** command configures the alarm triggering type, threshold for triggering an alarm and threshold for clearing an alarm based on the instance type and indicators of the threshold monitoring instance.

Prerequisites

Before the **threshold-alarm measure** command is run, run the **binding instance-type** *instance-type* { **all** | **instance** *instance-name* &<1-5> } command to bind a

threshold monitoring instance, and run the **threshold-alarm enable** command to enable the threshold alarm function. Otherwise, alarms will not be sent.

Example

Create threshold monitoring rules.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] binding instance-type ipfpm all
[HUAWEI-pm-statistics-task1] threshold-alarm enable
[HUAWEI-pm-statistics-task1] threshold-alarm measure forward-loss-ratio-max operation ge trigger-value 1000 clear-value 10
```

16.4.23 upload

Function

The **upload** command configures the device to upload performance statistics files to a PM server.

Format

upload *request-name* **file** *filename* &<1-16>

Parameters

Parameter	Description	Value
request-name	Specifies the name of a request for uploading performance statistics files.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.
file *filename*	Specifies the name of a performance statistics file.	The value is a string of 1 to 255 case-insensitive characters without spaces. The file name can contain the file path. If multiple files are specified, separate them with spaces.

Views

PM view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system periodically generates performance statistics files based on the collected performance statistics. You can manually upload the statistics files to a PM server.

Prerequisites

A request for uploading performance statistics files to the PM server has been created using the **upload-config** *request-name* **server** *server-name* command.

Follow-up Procedure

View the performance statistics on the PM server.

Example

Configure the device to upload performance statistics file to the PM server.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] pm-server ftpserver
[HUAWEI-pm-server-ftpserver] quit
[HUAWEI-pm] upload-config req1 server ftpserver
[HUAWEI-pm] upload req1 file stream20130703103001.txt
```

16.4.24 upload auto

Function

The **upload auto** command enables a device to automatically upload performance statistics files to a server.

The **undo upload auto** command disables a device from automatically uploading performance statistics files to a server.

By default, a device does not automatically upload performance statistics files to a server.

Format

upload auto *request-name*

undo upload auto

Parameters

Parameter	Description	Value
request-name	Specifies the name of a request for uploading performance statistics files to a server.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.

Views

Performance statistics collection task view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system periodically generates performance statistics files based on the collected performance statistics. To enable the device to automatically upload performance statistics files to the PM server at a specific interval, run the **upload auto** command.

Prerequisites

A request for uploading performance statistics files to the PM server has been created using the **upload-config** *request-name* **server** *server-name* command.

Example

Configure the device to automatically upload statistics files to a PM server.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] pm-server ftpserver
[HUAWEI-pm-server-ftpserver] quit
[HUAWEI-pm] upload-config req1 server ftpserver
[HUAWEI-pm] statistics-task task1
[HUAWEI-pm-statistics-task1] upload auto req1
```

16.4.25 upload-config

Function

The **upload-config** command creates a request for uploading performance statistics files to a specified PM server.

The **undo upload-config** command deletes a request for uploading performance statistics files to a specified PM server.

By default, no request for uploading performance statistics files is available on a device.

Format

upload-config *request-name* **server** *server-name*

undo upload-config *request-name*

Parameters

Parameter	Description	Value
request-name	Specifies the name of a request for uploading performance statistics files.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.
server *server-name*	Specifies the name of the process serving the PM server.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. The string contains letters, digits, and underscores (_), and must start with letters or digits.

Views

PM view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a device to upload performance statistics files to a PM server, run the **upload-config** command to create a file uploading request.

Prerequisites

A PM server process has been created using the **pm-server** *server-name* command.

Follow-up Procedure

Enable the device to upload performance statistics files to the PM server.

- Run the **upload** *request-name* **file** *filename* &<1-16> command in the PM view to manually upload statistics files to the PM server.
- Run the **upload auto** *request-name* command in the performance statistics collection task view to configure the device to automatically upload statistics files to the PM server.

Example

Create a request for uploading statistics files to a PM server.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] pm-server ftpserver
[HUAWEI-pm-server-ftpserver] quit
[HUAWEI-pm] upload-config req1 server ftpserver
```


16.4.26 username password

Function

The **username password** command configures the user name and password for logging in to the PM server.

The **undo username** command deletes the user name and password for logging in to the PM server.

By default, no user name and password for logging in to the PM server are configured.

Format

username *user-name* **password** *password*

undo username

Parameters

Parameter	Description	Value
user-name	Specifies the user name for logging in to a PM server.	The name is a string of 1 to 255 case-sensitive characters without spaces.
password	Specifies the password for logging in to a PM server.	The value is a string of 1 to 128 characters or a string of 32 to 200 characters. The password can be in plain or cipher text. • The password in plain text is a string of 1 to 128 case-sensitive characters without spaces. • The password in cipher text is a string of 32 to 200 characters. The password is displayed in ciphertext in the configuration file regardless of whether it is input in plain or cipher text. **NOTE** A 24-character ciphertext password configured in an earlier version is also supported in this version.

Views

PM server view

Default Level

2: Configuration level

Usage Guidelines

To log in to a PM server for upload performance statistics files to the PM server, run the **username password** command to configure the user name and password.

Example

Configure the user name and password for logging in to the PM server.

```
<HUAWEI> system-view
[HUAWEI] pm
[HUAWEI-pm] pm-server server1
[HUAWEI-pm-server-server1] username admin password Pwd@123
```

16.5 iPCA Configuration Commands

16.5.1 Command Support

Only the following switch models support iPCA:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S

16.5.2 ach

Function

The **ach** command creates an Atomic Closed Hop (ACH) and displays the ACH view. If the ACH already exists, the command displays the ACH view directly.

The **undo ach** command deletes an ACH and all configurations in the ACH view.

By default, no ACH is created.

Format

ach *ach-id*

undo ach *ach-id*

Parameters

Parameter	Description	Value
ach-id	Specifies an ACH ID.	The value is an integer ranging from 1 to 2147483647.

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACH consists of two target logical ports (TLPs) and is used to identify a segment between two specified devices on the network. In IP FPM hop-by-hop measurement, you need to specify the ACH for the target flow in a measurement instance and configure the direction and measurement points for the target flow in the ACH view. You can create an ACH and enter the ACH view by running the **ach** command.

Prerequisites

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

Example

Create an ACH.

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

16.5.3 authentication-mode (IPFPM-DCP view)

Function

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

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

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

Format

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

undo authentication-mode hmac-sha256

Parameters

Parameter	Description	Value
hmac-sha256	Uses HMAC-SHA256 to encrypt and authenticate packets sent by a DCP to the MCP.	-

Parameter	Description	Value
key-id *key-id*	Specifies the ID of the authentication password configured on a DCP.	The value is an integer that ranges from 1 to 64.
cipher	Specifies the cipher-text authentication password on a DCP.	-
password	Specifies the authentication password on a DCP.	The value is a case-sensitive character string without spaces. • The value is a string of 1 to 255 characters in plain text. • The value is a string of 32 to 392 characters in cipher text.

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

Prerequisites

Global DCP has been enabled using the **nqa ipfpm dcp** command.

Example

Configure the authentication mode and password on a DCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] authentication-mode hmac-sha256 key-id 1 cipher test12
```

16.5.4 authentication-mode (IPFPM-DCP instance view)

Function

The **authentication-mode** command configures the authentication mode and password for a measurement instance on a DCP.

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

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

Format

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

undo authentication-mode hmac-sha256

Parameters

Parameter	Description	Value
hmac-sha256	Uses HMAC-SHA256 to encrypt and authenticate packets sent by a DCP to the MCP.	-
key-id *key-id*	Specifies the ID of the authentication password configured for a measurement instance.	The value is an integer that ranges from 1 to 64.
cipher	Specifies the cipher-text authentication password for a measurement instance.	-
password	Specifies the authentication password for a measurement instance.	The value is a case-sensitive character string without spaces. • The value is a string of 1 to 255 characters in plain text. • The value is a string of 32 to 392 characters in cipher text.

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network demanding high security, when iPCA is used to measure network-level packet loss, enable authentication. After the same authentication mode and password are configured on the MCP and DCPs, the MCP accepts the packets only

from authenticated DCPs. This improves network security and reliability of packet loss measurement. The **authentication-mode** command configures the authentication mode and password for a measurement instance on a DCP.

Prerequisites

A measurement instance has been created on the DCP using the **instance** command.

Precautions

If the **authentication-mode** command is not used to configure the authentication mode and password, all measurement instances of the DCP use the authentication mode and password configured by the **authentication-mode (IPFPM-DCP view)** command.

Example

Configure the authentication mode and password for a measurement 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 test12
```

16.5.5 authentication-mode (IPFPM-MCP view)

Function

The **authentication-mode** command configures the authentication mode and password on the Measurement Control Point (MCP).

The **undo authentication-mode** command deletes the authentication mode and password on the MCP.

By default, no authentication mode or password is configured on the MCP.

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	Uses HMAC-SHA256 to decrypt and authenticate packets sent by a DCP to the MCP.	-
key-id *key-id*	Specifies the ID of the authentication password configured on the MCP.	The value is an integer that ranges from 1 to 64.

Parameter	Description	Value
cipher	Specifies the cipher-text authentication password configured on the MCP.	-
password	Specifies the authentication password configured on the MCP.	The value is a case-sensitive character string without spaces. • The value is a string of 1 to 255 characters in plain text. • The value is a string of 32 to 392 characters in cipher text.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network demanding high security, when iPCA is used to measure network-level packet loss, enable authentication. After the same authentication mode and password are configured on the MCP and DCPs, the MCP accepts the packets only from authenticated DCPs. This improves network security and reliability of packet loss measurement. The **authentication-mode** command configures the authentication mode and password on the MCP.

Prerequisites

Global MCP has been enabled using the **nqa ipfpm mcp** command.

Precautions

The MCP and DCP must be configured with the same authentication mode and password; otherwise, the MCP cannot obtain packet loss measurement from the DCP.

Example

Configure the authentication mode and password on the MCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] authentication-mode hmac-sha256 key-id 1 test12
```

16.5.6 color-flag loss-measure

Function

The **color-flag loss-measure** command configures the color bit used in network-level packet loss measurement.

The **undo color-flag** command restores the default color bit used in network-level packet loss measurement.

By default, bit 6 in the ToS field is used as the color bit for network-level packet loss measurement. The default configuration is recommended.

Format

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

undo color-flag

Parameters

Parameter	Description	Value
tos-bit *tos-bit*	Specifies a bit in the range of bits 3 to 7 in the ToS field of IP packets as the color bit for network-level packet loss measurement.	The value is an integer that ranges from 3 to 7.
flags-bit0	Specifies bit 0 in the Flags field of IP packets as the color bit for network-level packet loss measurement.	-

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before deploying Packet Conservation Algorithm for Internet (iPCA) to implement network-level packet loss measurement, run this command to configure the color bit. You can select a color bit according to the actual situation and network planning.

Prerequisites

Global DCP has been enabled using the **nqa ipfpm dcp** command.

Precautions

All devices on a network must use the same color bit setting. When the DS field is used to provide differentiated service, it is not recommended that you configure bits 3-5 as color bits because the measurement result may be inaccurate.

When both network-level and device-level packet loss measurements are enabled on a device, the color bits must be differentiated.

Example

Configure bit 3 in the ToS field as the color bit for network-level packet loss measurement.

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

16.5.7 dcp

Function

The **dcp** command associates the DCP ID with a measurement instance on the MCP.

The **undo dcp** command disassociates the DCP ID from a measurement instance on the MCP.

By default, no DCP ID is associated with a measurement instance on the MCP.

Format

dcp *dcp-id*

undo dcp [*dcp-id*]

Parameters

Parameter	Description	Value
dcp-id	Specifies the DCP ID to be associated with a measurement instance.	The value is in dotted decimal notation.

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Each measurement instance of the MCP contains one or more DCP IDs. The MCP checks whether the statistics data is complete based on the DCP ID, so the DCP ID must be specified for a measurement instance created on the MCP. The **dcp** command associates the DCP ID with a measurement instance on the MCP.

Prerequisites

A measurement instance has been created on the MCP using the **instance** command.

Precautions

The DCP ID associated with the measurement instance on the MCP must be the same as the DCP ID configured by the **dcp id** command on the DCP.

The **undo dcp** command without *dcp-id* specified deletes all DCP IDs associated with a measurement instance.

Example

Associate a DCP ID with measurement instance 1 on the 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
```

16.5.8 dcp id

Function

The **dcp id** command sets the DCP ID.

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

By default, no DCP ID is configured.

Format

dcp id *dcp-id*

undo dcp id

Parameters

Parameter	Description	Value
dcp-id	Specifies the DCP ID. It is recommended that you configure the router ID of the device as the DCP ID.	The value is in dotted decimal notation.

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the MCP communicates with a DCP, the DCP encapsulates statistics data collected from Target Logical Ports (TLPs) in a packet and sends the packet with the DCP ID as the source IP address. After receiving the packet sent from the DCP, the MCP compares the DCP ID in the packet with the DCP ID configured by the **dcp** command:

- If the two DCP IDs are the same, the MCP accepts the packet, and then summarizes and calculates the statistics data.
- If the two DCP IDs are different, the MCP considers the packet invalid and discards it.

Prerequisites

Global DCP has been enabled using the **nqa ipfpm dcp** command.

Precautions

Each DCP has a unique ID on the network. It is recommended that you configure the router ID of the device as the DCP ID. The DCP ID must be the same as the DCP ID in the measurement instance configured by the **dcp** command on the MCP.

Example

Set the DCP ID.

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

16.5.9 description (IPFPM-DCP instance view)

Function

The **description** command configures the description for a measurement instance on a DCP.

The **undo description** command deletes the description of a measurement instance on a DCP.

By default, no description is configured for a measurement instance on a DCP.

Format

description *text*

undo description

Parameters

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

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IP FPM instance is identified by an integer ID, and therefore its functions are not easy to understand. The **description** command configures the description for a measurement instance on a DCP, which helps you understand the function of the measurement instance.

It is recommended that the **description** command be used to configure the description for a measurement instance in the following situations:

- Many measurement instances are configured, and it is difficult to differentiate functions of each measurement instance.
- The interval for using the same measurement instance is too long, and functions of measurement instances change.

Precautions

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

Example

Configure the description for measurement instance 1.

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

16.5.10 description (IPFPM-MCP instance view)

Function

The **description** command configures the description for a measurement instance on the MCP.

The **undo description** command deletes the description of a measurement instance on the MCP.

By default, no description is configured for a measurement instance on the MCP.

Format

description *text*

undo description

Parameters

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

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IP FPM instance is identified by an integer ID, and therefore its functions are not easy to understand. The **description** command configures the description for a measurement instance on a DCP, which helps you understand the function of the measurement instance.

It is recommended that the **description** command be used to configure the description for a measurement instance in the following situations:

- Many measurement instances are configured, and it is difficult to differentiate functions of each measurement instance.
- The interval for using the same measurement instance is too long, and functions of measurement instances change.

Precautions

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

Example

Configure the description for measurement instance 1 on the MCP.

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

16.5.11 display ipfpm dcp

Function

The **display ipfpm dcp** command displays the DCP configuration in the IP Flow Performance Measurement (FPM) system.

Format

display ipfpm dcp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the DCP configuration.

Example

Display the DCP configuration.

```
<HUAWEI> display ipfpm dcp

Specification Information(Main Board):
 Max Instance Number                    : 512
 Max 10s Instance Number                : 512
 Max 1s Instance Number                 : 1
 Max TLP Number                         : 512
 Max TLP Number Per Instance            : 8

Configuration Information:
 DCP ID                          : 10.1.1.1
 Loss-measure Flag               : tos-bit6(default)
 Authentication Mode             : --
 Test Instances MCP ID           : 10.2.2.2
 Test Instances MCP Port         : 65030(default)
 Current Instance Number         : 1
```

Table 16-48 Description of the **display ipfpm dcp** command output

Item	Description
Specification Information(Main Board)	Specification information of the main board.
Max Instance Number	Maximum number of measurement instances supported.
Max 10s Instance Number	Maximum number of measurement instances at intervals of 10s.
Max 1s Instance Number	Maximum number of measurement instances at intervals of 1s.
Max TLP Number	Maximum number of TLPs supported.

Item	Description
Max TLP Number Per Instance	Maximum number of TLPs supported by each measurement instance.
Configuration Information	DCP configuration.
DCP ID	DCP ID. To configure this parameter, run the **dcp id** command.
Loss-measure Flag	Color bit used in packet loss measurement: • tos-bit3: bit 3 in the ToS field • tos-bit4: bit 4 in the ToS field • tos-bit5: bit 5 in the ToS field • tos-bit6: bit 6 in the ToS field • tos-bit7: bit 7 in the ToS field • flag-bit0: bit 0 in the Flags field To configure this parameter, run the **color-flag loss-measure** command.
Authentication Mode	Authentication mode on the DCP: • hmac-sha256: HMAC-SHA256 encrypted authentication • --: non-authentication To configure the authentication mode on a DCP, run the **authentication-mode** command.
Test Instances MCP ID	ID of the MCP corresponding to the DCP.
Test Instances MCP Port	UDP port number used by the DCP to communicate with the MCP.
Current Instance Number	Number of measurement instances.

16.5.12 display ipfpm mcp

Function

The **display ipfpm mcp** command displays the MCP configuration and status in the IP Flow Performance Measurement (FPM) system.

Format

display ipfpm mcp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the MCP configuration and status.

Example

Display the MCP configuration.

```
<HUAWEI> display ipfpm mcp
Specification Information:
 Max Instance Number                :128
 Max DCP Number Per Instance        :128
 Max ACH Number Per Instance        :36
 Max TLP Number Per ACH             :16

Configuration Information:
 MCP ID                             :10.1.1.1
 Status                             :Active
 Protocol Port                      :65030(default)
 Current Instance Number            :1
```

Table 16-49 Description of the display ipfpm mcp command output

Item	Description
Specification Information	Specifications of the MCP.
Max Instance Number	Maximum number of measurement instances supported by the MCP.
Max DCP Number Per Instance	Maximum number of DCPs supported by each measurement instance on the MCP.
Max ACH Number Per Instance	Maximum number of ACHs supported by each measurement instance on the MCP.
Max TLP Number Per ACH	Maximum number of TLPs supported by ACH on the MCP.
Configuration Information	MCP configuration.
MCP ID	MCP ID. To set the MCP ID, run the **mcp id** command on the MCP.

Item	Description
Status	MCP status: • Active: The MCP works properly. • Deleting: The **undo nqa ipfpm mcp** command is being used to disable global MCP.
Protocol Port	UDP port number through which the DCP and MCP communicate with each other. To configure the UDP port number through which the DCP and MCP communicate with each other, run the **protocol udp port** command.
Current Instance Number	Total number of measurement instances.

16.5.13 display ipfpm statistic-type

Function

The **display ipfpm statistic-type** command displays packet loss statistics of a specified measurement instance in the IP Flow Performance Measurement (FPM) system.

Format

display ipfpm statistic-type loss instance *instance-id* [**ach** *ach-id*]

Parameters

Parameter	Description	Value
loss	Displays packet loss statistics.	-
instance *instance-id*	Displays packet loss statistics of a specified measurement instance.	The value is an integer that ranges from 1 to 16777214.
ach *ach-id*	Displays hop-by-hop performance statistics for an Atomic Closed Hop (ACH).	The value is an integer ranging from 1 to 2147483647.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The packet loss statistics of a specified measurement instance include the indicators such as the number of discarded packets, number of discarded bytes, and packet loss ratio. To view packet loss statistics of a specified measurement instance, run the **display ipfpm statistic-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 can be only executed on the MCP.

The first statistics record obtained through the IP FPM may be inaccurate, so do not use the first statistics record to determine network performance.

If the packet loss ratio is a negative value, the service packets may be unknown unicast packets or the color bits on devices participating in measurement may be different.

Example

Display packet loss statistics of measurement instance 1.

```
<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%
```


Table 16-50 Description of the **display ipfpm statistic-type** command output

Item	Description
Latest loss statistics of forward flow	-
Latest loss statistics of backward flow	-
Period	Measurement interval.
Loss(p)	Number of discarded packets.
LossRatio(p)	Packet loss ratio.
Loss(b)	Number of discarded bytes.
LossRatio(b)	Packet loss ratio of bytes.

16.5.14 display iplpm configuration brief

Function

The **display iplpm configuration brief** command displays the brief configuration of device-level packet loss measurement (including measurement on the entire device and direct link).

Format

display iplpm configuration brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view parameters of device-level packet loss measurement, run this command.

Example

Display the brief configuration of device-level packet loss measurement.

```
<HUAWEI> display iplpm configuration brief
Configuration information:
```



```
------------------------------------------------------------------
Loss-measure flag               : flags-bit0(default)
Global loss-measure interval(s) : 10(default)
Global loss-measure status      : disable
Global loss-measure alarm       : disable
Loss-measure board number       : 1
Loss-measure board list         : 0
Loss-measure port number        : 9
Loss-measure port list          : GigabitEthernet0/0/1
                                  GigabitEthernet0/0/2
                                  GigabitEthernet0/0/3
                                  GigabitEthernet0/0/4
                                  GigabitEthernet0/0/5
                                  GigabitEthernet0/0/6
                                  GigabitEthernet0/0/7
                                  GigabitEthernet0/0/8
                                  GigabitEthernet0/0/9
------------------------------------------------------------------
```

Table 16-51 Description of the display iplpm configuration brief command output

Item	Description
Configuration information	Configuration of device-level packet loss measurement.
Loss-measure flag	Color bit for packet loss measurement. To configure the color bit, run the **iplpm loss-measure color-flag** command. ● tos-bit6: bit 6 in the ToS field ● tos-bit7: bit 7 in the ToS field ● flags-bit0: bit 0 in the Flags field The value default indicates that the default color bit is used.
Global loss-measure interval(s)	Measurement interval of packet loss measurement on the device. To set the measurement interval, run the **iplpm global loss-measure interval** command. The value default indicates that the default measurement interval is used.
Global loss-measure status	Whether packet loss measurement on the device is enabled. To packet loss measurement for a device, run the **iplpm global loss-measure enable** command. ● enable ● disable
Global loss-measure alarm	Whether the alarm and clear alarm of packet loss ratio are enabled. To enable the alarm and clear alarm of packet loss ratio, run the **iplpm global loss-measure alarm enable** command. ● enable ● disable

Item	Description
Loss-measure board number	Number of devices that support device-level packet loss measurement.
Loss-measure board list	List of slot numbers of devices that support device-level packet loss measurement. The value -- indicates that no device supports device-level packet loss measurement.
Loss-measure port number	Number of interfaces where packet loss measurement for direct links is enabled.
Loss-measure port list	List of interfaces where packet loss measurement for direct links is enabled. The value -- indicates that no interface is enabled with packet loss measurement for direct links.

16.5.15 display iplpm loss-measure statistics global

Function

Run the **display iplpm loss-measure statistics global** command displays the packet loss measurement result on a device.

Format

display iplpm loss-measure statistics global

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the packet loss measurement result on a device, including the number of discarded packets, packet loss ratio, and error information.

Example

Display the packet loss measurement result on a device.

```
<HUAWEI> display iplpm loss-measure statistics global
Latest global loss statistics:
```



```
-------------------------------------------------------------------------------
StartTime(DST)       Loss Packets        LossRatio       ErrorInfo
-------------------------------------------------------------------------------
2014-06-12 18:47:30  344127              4.513519%       OK
2014-06-12 18:47:20  381085              4.513196%       OK
2014-06-12 18:47:10  381192              4.513290%       OK
2014-06-12 18:47:00  381339              4.513341%       OK
2014-06-12 18:46:50  381465              4.513392%       OK
2014-06-12 18:46:40  381444              4.513487%       OK
2014-06-12 18:46:30  381129              4.513309%       OK
-------------------------------------------------------------------------------
```

Table 16-52 Description of the **display iplpm loss-measure statistics global** command output

Item	Description
Latest global loss statistics	Latest statistics about packet loss measurement on the device.
StartTime(DST)	Time the packet loss measurement result was generated (standard DST), which is also the start time of each measurement interval.
Loss Packets	Number of discarded packets in the current measurement interval.
LossRatio	Packet loss ratio in the current measurement interval.
ErrorInfo	Error code about packet loss measurement in the current measurement interval: • OK: There is no error, and the packet loss measurement result is normal. • Incomplete: The statistics data is incomplete. The possible reason is the inter-chassis communication error. Part of statistics on the standby or slave switch cannot be sent to the master switch.

16.5.16 display iplpm loss-measure statistics history-record

Function

The **display iplpm loss-measure statistics history-record** command displays the historical records of packet loss measurement on a device and a direct link.

Format

display iplpm loss-measure statistics history-record { **global** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
global	Displays the historical records of packet loss measurement on a device.	-
interface *interface-type interface-number*	Displays the historical records of packet loss measurement on a direct link.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the measurement interval is 1s, 10s, or 60s, the system summarizes statistics results in each measurement interval every 5 minutes to obtain the maximum and minimum packet loss ratios within 5 minutes. When the measurement interval is 600s, the system summarizes statistics results in each measurement interval every 60 minutes to obtain the maximum and minimum packet loss ratios within 60 minutes. The system saves a maximum of four summarized records. You can run this command to view historical records.

Example

Display the historical records of packet loss measurement on a device.

```
<HUAWEI> display iplpm loss-measure statistics history-record global
Latest global history record(every 5 minutes):
------------------------------------------------------------------------------
 Record no                    : 29
 Period(DST)                  : 2014-03-19 16:20:10 to 2014-03-19 16:25:10
 Valid statistic data number  : 30
 Maximum loss ratio           : 0.000000%
 Minimum loss ratio           : 0.000000%
 Total loss packets           : 0
 Total receive packets        : 0

 Record no                    : 28
 Period(DST)                  : 2014-03-19 16:15:10 to 2014-03-19 16:20:10
 Valid statistic data number  : 30
 Maximum loss ratio           : 0.000000%
 Minimum loss ratio           : 0.000000%
 Total loss packets           : 0
 Total receive packets        : 0

 Record no                    : 27
 Period(DST)                  : 2014-03-19 16:10:10 to 2014-03-19 16:15:10
 Valid statistic data number  : 30
 Maximum loss ratio           : 0.000000%
 Minimum loss ratio           : 0.000000%
 Total loss packets           : 0
 Total receive packets        : 0
```



```
 Record no                    : 26
 Period(DST)                  : 2014-03-19 16:05:10 to 2014-03-19 16:10:10
 Valid statistic data number  : 30
 Maximum loss ratio           : 0.000000%
 Minimum loss ratio           : 0.000000%
 Total loss packets           : 0
 Total receive packets        : 0

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

Display the historical records of packet loss measurement on a direct link of GE0/0/1.

```
<HUAWEI> display iplpm loss-measure statistics history-record interface gigabitethernet 0/0/1
Latest history record of interface GigabitEthernet0/0/1(every 5 minutes):
------------------------------------------------------------------------------
 Record no                    : 29
 Period(DST)                  : 2014-03-19 16:20:10 to 2014-03-19 16:25:10
 Valid statistic data number  : 30
 Maximum forward loss ratio   : 0.000000%
 Minimum forward loss ratio   : 0.000000%
 Total forward loss packets   : 0
 Total forward receive packets : 0
 Maximum backward loss ratio  : 20.000000%
 Minimum backward loss ratio  : 19.980020%
 Total backward loss packets  : 6000
 Total backward receive packets : 30001

 Record no                    : 28
 Period(DST)                  : 2014-03-19 16:15:10 to 2014-03-19 16:20:10
 Valid statistic data number  : 30
 Maximum forward loss ratio   : 0.000000%
 Minimum forward loss ratio   : 0.000000%
 Total forward loss packets   : 0
 Total forward receive packets : 0
 Maximum backward loss ratio  : 20.079920%
 Minimum backward loss ratio  : 19.980020%
 Total backward loss packets  : 6001
 Total backward receive packets : 30003

 Record no                    : 27
 Period(DST)                  : 2014-03-19 16:10:10 to 2014-03-19 16:15:10
 Valid statistic data number  : 30
 Maximum forward loss ratio   : 0.000000%
 Minimum forward loss ratio   : 0.000000%
 Total forward loss packets   : 0
 Total forward receive packets : 0
 Maximum backward loss ratio  : 20.039880%
 Minimum backward loss ratio  : 19.960080%
 Total backward loss packets  : 6001
 Total backward receive packets : 30005

 Record no                    : 26
 Period(DST)                  : 2014-03-19 16:05:10 to 2014-03-19 16:10:10
 Valid statistic data number  : 30
 Maximum forward loss ratio   : 0.000000%
 Minimum forward loss ratio   : 0.000000%
 Total forward loss packets   : 0
 Total forward receive packets : 0
 Maximum backward loss ratio  : 20.059880%
 Minimum backward loss ratio  : 19.980020%
 Total backward loss packets  : 6001
 Total backward receive packets : 30004
------------------------------------------------------------------------------
```

Table 16-53 Description of the **display iplpm loss-measure statistics history-record** command output

Item	Description
Latest global history record(every 5 minutes)	Latest statistics about packet loss measurement in every five minutes on the device.
Latest history record of interface *x* (every 5 minutes)	Latest statistics about packet loss measurement on a direct link of the *x* interface in every five minutes.
Record no	Historical record ID.
Period(DST)	Time historical records were generated (standard DST).
Valid statistic data number	Number of valid historical statistics records.
Maximum loss ratio	Maximum packet loss ratio of the device.
Minimum loss ratio	Minimum packet loss ratio of the device.
Total loss packets	Total number of packets discarded by the device.
Total receive packets	Total number of packets received by the device.
Maximum forward loss ratio	Maximum packet loss ratio of a forward flow (a forward flow is sent by the local device interface and received by the remote device interface).
Minimum forward loss ratio	Minimum packet loss ratio of a forward flow.
Total forward loss packets	Total number of discarded packets of a forward flow.
Total forward receive packets	Total number of received packets (including the number of discarded packets) of a forward flow.
Maximum backward loss ratio	Maximum packet loss ratio of a backward flow (a backward flow is sent by the remote device interface and received by the local device interface).
Minimum backward loss ratio	Minimum packet loss ratio of a backward flow.
Total backward loss packets	Total number of discarded packets of a backward flow.
Total backward receive packets	Total number of received packets (including the number of discarded packets) of a backward flow.

16.5.17 display iplpm loss-measure statistics interface

Function

The **display iplpm loss-measure statistics interface** command displays the packet loss measurement result on the direct link of a specified interface.

Format

display iplpm loss-measure statistics interface *interface-type interface-number* [**forward** | **backward**]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays the packet loss measurement result on the direct link of a specified interface.	-
forward	Displays the packet loss measurement result of a forward flow on the direct link of a specified interface. A forward flow is sent by the local device interface and received by the remote device interface.	-
backward	Displays the packet loss measurement result of a backward flow on the direct link of a specified interface. A backward flow is sent by the remote device interface and received by the local device interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the packet loss measurement result in the forward and backward directions, including the number of discarded packets and packet loss ratio.

Example

Display the packet loss measurement result on the direct link of GE0/0/1.

```
<HUAWEI> display iplpm loss-measure statistics interface gigabitethernet 0/0/1
Latest forward loss statistics of interface GigabitEthernet0/0/1:
------------------------------------------------------------------------------------------------

 StartTime(DST)       Forward Loss Packets  Forward LossRatio
ErrorInfo
------------------------------------------------------------------------------------------------
```



```
2014-03-19 15:50:50   200              19.980020%        OK
2014-03-19 15:50:40   200              20.000000%        OK
2014-03-19 15:50:30   200              19.980020%        OK
2014-03-19 15:50:20   200              20.020020%        OK
2014-03-19 15:50:10   200              20.000000%        OK
2014-03-19 15:50:00   200              19.980020%        OK
-------------------------------------------------------------------------------------------------------
Latest backward loss statistics of interface
GigabitEthernet0/0/1:
-------------------------------------------------------------------------------------------------------

 StartTime(DST)       Backward Loss Packets  Backward LossRatio
ErrorInfo
-------------------------------------------------------------------------------------------------------

2014-03-19 15:50:50   0                0.000000%         OK
2014-03-19 15:50:40   0                0.000000%         OK
2014-03-19 15:50:30   0                0.000000%         OK
2014-03-19 15:50:20   0                0.000000%         OK
2014-03-19 15:50:10   0                0.000000%         OK
2014-03-19 15:50:00   0                0.000000%         OK
-------------------------------------------------------------------------------------------------------
```

Table 16-54 Description of the **display iplpm loss-measure statistics interface** command output

Item	Description
Latest forward loss statistics of interface *x*	Latest statistics about packet loss measurement of a forward target flow on the direct link of the *x* interface (a forward flow is sent by the local device interface and received by the remote device interface).
Latest backward loss statistics of interface *x*	Latest statistics about packet loss measurement of a backward target flow on the direct link of the *x* interface (a backward flow is sent by the remote device interface and received by the local device interface).
StartTime(DST)	Time the packet loss measurement result was generated (standard DST), which is also the start time of each measurement interval.
Forward Loss Packets	Number of discarded packets of a forward flow in the current measurement interval.
Forward LossRatio	Packet loss ratio of a forward flow in the current measurement interval.
Backward Loss Packets	Number of discarded packets of a backward flow in the current measurement interval.
Backward LossRatio	Packet loss ratio of a backward flow in the current measurement interval.

Item	Description
ErrorInfo	Error code about packet loss measurement in the current measurement interval: ● Init: The device is in initialized state and there is no statistics data. ● OK: There is no error, and the packet loss measurement result is normal. ● NoRecvData: The local end does not receive statistics data from the remote end. The possible causes may be that the packet loss measurement on a direct link is not enabled on the remote device or the direct link becomes faulty or there is a forwarding node on the link. ● DataErr: The local end receives error statistics data from the remote end. ● DiffAuth: The authentication modes or passwords on both ends are different. ● DiffIntvl: The measurement intervals on both ends are different. ● ASynClock: The time on both ends is asynchronous. When this code occurs, check the NTP configuration. ● PortIsDown: The interface is Down.

16.5.18 display iplpm loss-measure statistics port-flow interface

Function

The **display iplpm loss-measure statistics port-flow interface** command displays statistics about discarded packets on an interface.

Format

display iplpm loss-measure statistics port-flow interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Displays statistics about discarded packets on a specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you find packet loss on an interface in the packet loss measurement result on the direct link in the **display iplpm loss-measure statistics interface** command output, you can run the **display iplpm loss-measure statistics port-flow interface** command to check the statistics data. Then you can check whether the fault on the local interface causes packet loss.

Example

Display statistics about discarded packets on GE0/0/1.

```
<HUAWEI> display iplpm loss-measure statistics port-flow interface gigabitethernet 0/0/1
Latest port loss statistics of interface GigabitEthernet0/0/1:
--------------------------------------------------------------------------------
 StartTime(DST)        Output Packets Loss Ratio     Input Packets Loss Ratio
--------------------------------------------------------------------------------
 2014-04-01 18:09:40   0.000000%                     0.000000%
 2014-04-01 18:09:30   0.000000%                     0.000000%
 2014-04-01 18:09:20   0.000000%                     0.000000%
 2014-04-01 18:09:10   0.000000%                     0.000000%
--------------------------------------------------------------------------------
```

Table 16-55 Description of the **display iplpm loss-measure statistics port-flow interface** command output

Item	Description
Latest port loss statistics of interface *x*	Latest statistics about packet loss measurement on the *x* interface.
StartTime(DST)	Time the packet loss measurement result was generated (standard DST), which is also the start time of each measurement interval.
Output Packets Loss Ratio	Packet loss rate of packets sent from the local interface and received by the peer interface during the current statistics interval.
Input Packets Loss Ratio	Packet loss rate of packets sent from the peer interface and received by the local interface during the current statistics interval.

16.5.19 display iplpm loss-measure statistics qos-queue interface

Function

The **display iplpm loss-measure statistics qos-queue interface** command displays statistics about sent packets in QoS queues on an interface.

Format

display iplpm loss-measure statistics qos-queue interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Displays statistics about sent packets in QoS queues on a specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you find packet loss on an interface in the packet loss measurement result on the direct link in the **display iplpm loss-measure statistics interface** command output, you can run the **display iplpm loss-measure statistics qos-queue interface** command to check the statistics about sent packets in QoS queues on an interface. Then you can check whether congestion in queues causes packet loss.

Example

Display statistics about sent packets in QoS queues on GE0/0/1.

```
<HUAWEI> display iplpm loss-measure statistics qos-queue interface gigabitethernet 0/0/1
Latest qos queue loss statistics of interface
GigabitEthernet0/0/1:
------------------------------------------------------------------------------

StartTime(DST): 2014-03-19 16:25:10
 Queue0   : 0.000000%          Queue1: 0.000000%
 Queue2   : 0.000000%          Queue3: 0.000000%
 Queue4   : 0.000000%          Queue5: 0.000000%
 Queue6   : 0.000000%          Queue7: 0.000000%
 UserQueue: 0.000000%

StartTime(DST): 2014-03-19 16:25:00
 Queue0   : 0.000000%          Queue1: 0.000000%
```



```
Queue2   : 0.000000%        Queue3: 0.000000%
Queue4   : 0.000000%        Queue5: 0.000000%
Queue6   : 0.000000%        Queue7: 0.000000%
UserQueue: 0.000000%

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

Table 16-56 Description of the display iplpm loss-measure statistics qos-queue interface command output

Item	Description
StartTime(DST)	Time the packet loss measurement result was generated (standard DST), which is also the start time of each measurement interval.
Queue0-Queue7	Packet loss ratios of queues 0 to 7 in the measurement interval, which is used for reference only.
UserQueue	Packet loss ratio of the subscriber queue on the interface in the current measurement interval. The value of this field can be obtained only when HQoS is configured, and is used for reference only.

16.5.20 flow (IPFPM-DCP instance view)

Function

The **flow** command configures a target flow in a measurement instance on a DCP.

The **undo flow** command deletes the target flow from a measurement instance on a DCP.

By default, no target flow is configured in a measurement instance on a DCP.

Format

Define a unidirectional flow.

- When the protocol of a target flow is TCP or UDP, run the following command:

  flow { **forward** | **backward** } { **protocol** { **tcp** | **udp** } { **source-port** *src-port-number1* [**to** *src-port-number2*] | **destination-port** *dest-port-number1* [**to** *dest-port-number2*] } * | **dscp** *dscp-value* | **source** *src-ip-address* [*src-mask-length*] | **destination** *dest-ip-address* [*dest-mask-length*] } *
- When the protocol of a target flow is not TCP or UDP, run the following command:

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

Define a bidirectional symmetrical flow.

- When the protocol of a target flow is TCP or UDP, run the following command:

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

- When the protocol of a target flow is not TCP or UDP, run the following command:

  flow bidirectional { **protocol** *protocol-number* | **dscp** *dscp-value* | **source** *src-ip-address* [*src-mask-length*] | **destination** *dest-ip-address* [*dest-mask-length*] } *

Cancel the configured target flow.

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

Parameters

Parameter	Description	Value
forward	Indicates the forward flow.	-
backward	Indicates the backward flow.	-
protocol { **tcp** | **udp** }	Indicates that the protocol of a target flow is TCP or UDP.	-
source-port *src-port-number1*	Specifies the start source port number of a target flow.	The value is an integer that ranges from 1 to 65535.
src-port-number2	Specifies the end source port number of a target flow.	The value is an integer that ranges from 1 to 65535. *src-port-number2* must be larger than *src-port-number1*.
destination-port *dest-port-number1*	Specifies the start destination port number of a target flow.	The value is an integer that ranges from 1 to 65535.
dest-port-number2	Specifies the end destination port number of a target flow.	The value is an integer that ranges from 1 to 65535. *dest-port-number2* must be larger than *dest-port-number1*.
dscp *dscp-value*	Specifies the value of a Differentiated Services CodePoint (DSCP) of a target flow.	The value is an integer that ranges from 0 to 63.
source *src-ip-address*	Specifies the source IP address of a target flow. Only unicast IP addresses are supported.	The value is in dotted decimal notation.

Parameter	Description	Value
src-mask-length	Specifies the mask length of the source IP address of a target flow.	The value is an integer that ranges from 1 to 32.
destination *dest-ip-address*	Specifies the destination IP address of a target flow. Only unicast IP addresses are supported.	The value is in dotted decimal notation.
dest-mask-length	Specifies the mask length of the destination IP address of a target flow.	The value is an integer that ranges from 1 to 32.
protocol *protocol-number*	Specifies the protocol type of a 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.
bidirectional	Indicates the bidirectional symmetrical 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.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The target flow must be specified before each measurement.

A target flow is the objective in iPCA measurement, and can be defined by any combinations of source IP address, destination IP address, protocol type, DSCP value, source port number, and destination port number. Specifying more attributes can make the target flow accurate. Therefore, it is recommended that you specify more attributes to improve precision of measurement results.

Precautions

An 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 instance is unidirectional, you can specify **forward** to configure a forward flow or **backward** to configure a backward flow.
- If the target flow in an 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, and you must specify the source and destination IP addresses. 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.

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.

Example

Configure a target flow of measurement instance 1 on a DCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] instance 1
[HUAWEI-nqa-ipfpm-dcp-instance-1] flow bidirectional protocol udp source-port 1025 source 10.1.1.1 destination 10.2.2.2
```

16.5.21 flow (IPFPM-MCP-ACH view)

Function

The **flow** command configures the target flow direction in the Atomic Closed Hop (ACH) view.

The **undo flow** command deletes the target flow direction in the ACH view.

By default, no direction is configured for target flows in the ACH view.

Format

flow { **forward** | **backward** }

undo flow

Parameters

Parameter	Description	Value
forward	Indicates the forward target flow.	-
backward	Indicates the backward target flow.	-

Views

IPFPM-MCP-ACH view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **flow** command in IP FPM hop-by-hop performance statistics scenarios.

Prerequisites

The **ach** command has been run to create an ACH and display the ACH view.

Example

Configure the forward target flow in the ACH view.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] ach 1
[HUAWEI-nqa-ipfpm-mcp-instance-1-ach-1] flow forward
```

16.5.22 in-group

Function

The **in-group** command creates a Target Logical Port (TLP) in-group for the target flow.

The **undo in-group** command deletes a TLP in-group or deletes a TLP from a TLP in-group.

By default, no TLP in-group is configured for the target flow.

Format

in-group dcp *dcp-id* **tlp** *tlp-id*

undo in-group [**dcp** *dcp-id* **tlp** *tlp-id*]

Parameters

Parameter	Description	Value
dcp *dcp-id*	Specifies a DCP to which TLPs in a TLP in-group belongs.	This value is in dotted decimal notation.
tlp *tlp-id*	Indicates a TLP in a TLP in-group.	The value is an integer ranging from 1 to 16777215.

Views

IPFPM-MCP-ACH view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In IP FPM hop-by-hop performance statistics scenarios, a hop is a set of links and interfaces that service packets travel through, from one measurement point or group to the next measurement point or group, and therefore is represented by (TLP in-group, TLP out-group). Performance statistics are implemented on the TLP in-point or in-group through which service packets enter a network and the TLP out-point or out-group through which service packets leave the network.

Prerequisites

The **ach** command has been run to create an ACH and display the ACH view.

Example

Create a TLP in-group for the target flow.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] ach 1
[HUAWEI-nqa-ipfpm-mcp-instance-1-ach-1] in-group dcp 10.1.1.1 tlp 100
```

16.5.23 instance (IPFPM-DCP view)

Function

The **instance** command creates an IPFPM-DCP instance and displays the IPFPM-DCP instance view, or directly displays the view of an existing IPFPM-DCP instance.

The **undo instance** command deletes an IPFPM-DCP instance.

By default, no IPFPM-DCP instance is created on a DCP.

Format

instance *instance-id*

undo instance *instance-id*

Parameters

Parameter	Description	Value
instance-id	Specifies the ID of an IPFPM-DCP instance.	The value is an integer that ranges from 1 to 8355838.

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DCP collects statistics data based on measurement instances. Each measurement instance consists of the target flow, TLP, and measurement interval. The MCP reports measurement results based on measurement instances. The MCP summarizes and analyzes statistics data of the same measurement instance on all DCPs, and reports measurement results of target flows.

Prerequisites

Global DCP has been enabled using the **nqa ipfpm dcp** command.

Follow-up Procedure

Run the **flow** command to configure a target flow, run the **tlp** command to configure the TLPs of the measurement instance, and run the **interval** command to configure the measurement interval.

Precautions

To measure packet loss for a specified service flow, create the same measurement instance on the MCP and DCP.

Example

Create IPFPM-DCP instance 1.

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


16.5.24 instance (IPFPM-MCP view)

Function

The **instance** command creates an IPFPM-MCP instance and displays the IPFPM-MCP instance view, or directly displays the view of an existing IPFPM-MCP instance.

The **undo instance** command deletes an IPFPM-MCP instance.

By default, no IPFPM-MCP instance is created on the MCP.

Format

instance *instance-id*

undo instance *instance-id*

Parameters

Parameter	Description	Value
instance-id	Specifies the ID of an IPFPM-MCP instance.	The value is an integer that ranges from 1 to 8355838.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DCP collects statistics data based on measurement instances. Each measurement instance consists of the target flow, TLP, and measurement interval. The MCP reports measurement results based on measurement instances. The MCP summarizes and analyzes statistics data of the same measurement instance on all DCPs, and reports measurement results of target flows.

Prerequisites

Global MCP has been enabled using the **nqa ipfpm mcp** command.

Precautions

To measure packet loss for a specified service flow, create the same measurement instance on the MCP and DCP.

Example

Create IPFPM-MCP instance 1.


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

16.5.25 interval (IPFPM-DCP instance view)

Function

The **interval** command sets the measurement interval of a measurement instance on a DCP.

The **undo interval** command restores the default measurement interval of a measurement instance on a DCP.

By default, the measurement interval of a measurement instance on a DCP is 10 seconds.

Format

interval *interval*

undo interval

Parameters

Parameter	Description	Value
interval	Specifies the measurement interval of a measurement instance on a DCP.	The value is of the enumerated type and can be 1, 10, 60, or 600, in seconds.

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The measurement interval of a measurement instance on a DCP is the interval at which a TLP collects statistics on packets or bytes and records the timestamp of packet receiving or sending. It is also the interval at which a DCP reports statistics data to the MCP. A shorter interval indicates a higher frequency at which a DCP reports statistics data to the MCP, so the interval adjustment affects the performance of the DCP and MCP.

Considering factors such as the clock synchronization offset, maximum transmission delay, and device performance, you can run this command to change the measurement interval.

Precautions

The measurement intervals of the same measurement instances on all DCPs must be the same; otherwise, the statistics data will be empty.

The measurement interval of a measurement instance cannot be changed when the measurement instance is running. If the measurement interval of a running measurement instance is changed, the statistics reported by MCP may be inaccurate. To change the measurement interval, run the **measure disable** command in the IPFPM-MCP instance view to disable the measurement, and then run the **measure enable** command to enable the measurement.

Example

Set the measurement interval of measurement instance 1 to 60s.

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

16.5.26 ipfpm tlp

Function

The **ipfpm tlp** command binds a Target Logical Port (TLP) to an interface in a measurement instance on a DCP.

The **undo ipfpm tlp** command unbinds a TLP from an interface in a measurement instance on a DCP.

By default, an interface is not bound to a TLP in a measurement instance on a DCP.

Format

ipfpm tlp *tlp-id*

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

Parameters

Parameter	Description	Value
tlp-id	Specifies the ID of a TLP.	The value is an integer that ranges from 1 to 16777215.
all	Cancels the binding between all TLPs and interfaces.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before performing packet loss measurement, run this command to bind a TLP to an interface.

Prerequisites

A Layer 2 or Layer 3 interface can be bound to a TLP. You can run the **undo portswitch** command to switch the interface to Layer 3 mode.

Precautions

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

Example

Bind GE0/0/1 to TLP 100.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] ipfpm tlp 100
```

16.5.27 iplpm global loss-measure alarm enable

Function

The **iplpm global loss-measure alarm enable** command enables the alarm and clear alarm of the packet loss ratio for device-level packet loss measurement.

The **undo iplpm global loss-measure alarm enable** command restores the default setting.

By default, the alarm and clear alarm of the packet loss ratio are disabled.

Format

iplpm global loss-measure alarm enable

undo iplpm global loss-measure alarm enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After this command is used, the alarm threshold and clear alarm threshold of the packet loss ratio are 5% and 1%.

- If the packet loss ratio in five consecutive measurement intervals exceeds the alarm threshold, the device reports the hwIpfpmLossRatioExceed alarm to the NMS to notify the link fault in real time.
- If the packet loss ratio in five consecutive measurement intervals falls below or is equivalent to the clear alarm threshold, the device reports the hwIpfpmLossRatioRecovery alarm to the NMS to notify link recovery in real time.

Example

Enable the alarm and clear alarm of the packet loss ratio for device-level packet loss measurement.

```
<HUAWEI> system-view
[HUAWEI] iplpm global loss-measure alarm enable
```

16.5.28 iplpm global loss-measure enable

Function

The **iplpm global loss-measure enable** command enables packet loss measurement for a device.

The **undo iplpm global loss-measure enable** command disables packet loss measurement for a device.

By default, packet loss measurement for a device is disabled.

Format

iplpm global loss-measure enable

undo iplpm global loss-measure enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To measure the packet loss of a switch, run this command to enable packet loss measurement for the switch.

Example

Enable packet loss measurement for a device.

```
<HUAWEI> system-view
[HUAWEI] iplpm global loss-measure enable
```

16.5.29 iplpm global loss-measure interval

Function

The **iplpm global loss-measure interval** command configures the device-level packet loss measurement interval.

The **undo iplpm global loss-measure interval** command restores the default device-level packet loss measurement interval.

By default, the device-level packet loss measurement interval is 10s.

Format

iplpm global loss-measure interval *interval*

undo iplpm global loss-measure interval

Parameters

Parameter	Description	Value
interval	Specifies the device-level packet loss measurement interval.	The value is of the enumerated type and can be 1, 10, 60, or 600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device-level packet loss measurement interval refers to the period from received packet statistics collection to sent packet statistics collection. To ensure accuracy of statistics data, run the **undo iplpm global loss-measure enable** command to disable device-level packet loss measurement in the system view before changing the measurement interval.

Example

Set the device-level packet loss measurement interval to 60s.


```
<HUAWEI> system-view
[HUAWEI] iplpm global loss-measure interval 60
```

16.5.30 iplpm link authentication-mode

Function

The **iplpm link authentication-mode** command configures the authentication mode and password for packet loss measurement on a direct link.

The **undo iplpm link authentication-mode** command deletes the authentication mode and password.

By default, no authentication mode or password is configured for packet loss measurement on a direct link.

Format

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

undo iplpm link authentication-mode

Parameters

Parameter	Description	Value
hmac-sha256	Uses HMAC-SHA256 to authenticate packets between devices.	-
key-id *key-id*	Specifies the ID of the authentication password.	The value is an integer that ranges from 1 to 64.
cipher	Specifies the cipher-text authentication password.	-
password	Specifies the authentication password.	The value is a character string without spaces. • The value is a string of 1 to 255 characters in plain text. • The value is a string of 32 to 392 characters in cipher text.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After packet loss measurement is configured on a direct link, statistics data on received and sent packets on an interface at one end is sent to an interface at the other end and summarized for packet loss measurement. This command is used to authenticate communication packets on the direct link, improving security.

Precautions

- When the authentication mode and password are configured on an interface, packets encapsulated with local statistics data sent from the interface are authenticated. Therefore, both interfaces of the direct link must be configured with the same authentication mode and password.
- For security purposes, it is recommended that the authentication password contain at least 16 characters.

Example

Set the authentication mode to hmac-sha256 and password to **YsHsjx_202206** in cipher text for packet loss measurement on a direct link on the GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] iplpm link authentication-mode hmac-sha256 key-id 1 cipher YsHsjx_202206
```

16.5.31 iplpm link loss-measure alarm enable

Function

The **iplpm link loss-measure alarm enable** command enables the alarm and clear alarm of the packet loss ratio for packet loss measurement on a direct link.

The **undo iplpm link loss-measure alarm enable** command restores the default setting.

By default, the packet loss alarm and clear alarm are disabled for packet loss measurement on a direct link.

Format

iplpm link loss-measure alarm enable

undo iplpm link loss-measure alarm enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

After this command is used, the alarm threshold and clear alarm threshold of the packet loss ratio are 5% and 1%.

- If the packet loss ratio in five consecutive measurement intervals exceeds the alarm threshold, the device reports the hwIpfpmLossRatioExceed alarm to the NMS to notify the link fault in real time.
- If the packet loss ratio in five consecutive measurement intervals falls below the clear alarm threshold, the device reports the hwIpfpmLossRatioRecovery alarm to the NMS to notify link recovery in real time.

Example

On the GE0/0/1, enable the alarm and clear alarm of the packet loss ratio for packet loss measurement on a direct link.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] iplpm link loss-measure alarm enable
```

16.5.32 iplpm link loss-measure enable

Function

The **iplpm link loss-measure enable** command enables packet loss measurement on the direct link.

The **undo iplpm link loss-measure enable** command disables packet loss measurement on the direct link.

By default, packet loss measurement is disabled on the direct link.

Format

iplpm link loss-measure enable

undo iplpm link loss-measure enable

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

To accurately locate packet loss on a link, run the **iplpm link loss-measure enable** command to enable packet loss measurement on the direct link between two devices.

This function must be enabled on both device interfaces of the direct link.

Example

On the GE0/0/1, enable packet loss measurement on the direct link.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] iplpm link loss-measure enable
```

16.5.33 iplpm link loss-measure interval

Function

The **iplpm link loss-measure interval** command configures the interval for packet loss measurement on the direct link.

The **undo iplpm link loss-measure interval** command restores the default interval for packet loss measurement on the direct link.

By default, the interval for packet loss measurement on the direct link is 10s.

Format

iplpm link loss-measure interval *interval*

undo iplpm link loss-measure interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for packet loss measurement on the direct link.	The value is an integer that can be 1, 10, 60, or 600, in seconds.

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view

Default Level

2: Configuration level

Usage Guidelines

The interval for packet loss measurement on the direct link refers to the period from received packet statistics collection to sent packet statistics collection on a

specified interface. To ensure accuracy of statistics data, run the **undo iplpm link loss-measure enable** command to disable packet loss measurement on the direct link in the interface view before changing the measurement interval.

Example

On the GE0/0/1, set the interval for packet loss measurement on the direct link to 60s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] iplpm link loss-measure interval 60
```

16.5.34 iplpm loss-measure color-flag

Function

The **iplpm loss-measure color-flag** command configures the color bit used in device-level packet loss measurement.

The **undo iplpm loss-measure color-flag** command restores the default color bit used in device-level packet loss measurement.

By default, bit 0 in the Flags field is used as the color bit for device-level packet loss measurement. The default configuration is recommended.

Format

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

undo iplpm loss-measure color-flag

Parameters

Parameter	Description	Value
tos-bit *tos-bit*	Specifies bit 6 or 7 in the ToS field of IP packets as the color bit for device-level packet loss measurement.	The value is 6 or 7.
flags-bit0	Specifies bit 0 in the Flags field of IP packets as the color bit for device-level packet loss measurement.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Device-level packet loss measurement contains measurement on the entire device and direct link. Before deploying Packet Conservation Algorithm for Internet (iPCA) to implement device-level packet loss measurement, run this command to configure the color bit. You can select a color bit according to the actual situation and network planning.

Precautions

Before changing the color bit for device-level packet loss measurement, run the **undo iplpm global loss-measure enable** command in the system view to disable device-level packet loss measurement. If packet loss measurement is configured on the direct link, run the **undo iplpm link loss-measure enable** command in the interface view to disable packet loss measurement on the direct link and ensure that the color bits on both devices of the direct link are changed to be the same.

When both network-level and device-level packet loss measurements are enabled on a device, the color bits must be differentiated.

Example

Configure bit 7 in the ToS field as the color bit for device-level packet loss measurement.

```
<HUAWEI> system-view
[HUAWEI] iplpm loss-measure color-flag tos-bit 7
```

16.5.35 loss-measure enable

Function

The **loss-measure enable** command enables statistics collection based on the time range for a measurement instance on a DCP.

The **undo loss-measure enable** command disables statistics collection for a measurement instance on a DCP.

By default, statistics collection based on the time range is disabled for a measurement instance on a DCP.

Format

loss-measure enable [**mid-point**] [**time-range** *time-range*]

undo loss-measure enable [[**mid-point**] **time-range** [*time-range*]]

Parameters

Parameter	Description	Value
mid-point	Enables on-demand packet loss measurement for mid-points. If this parameter is configured, on-demand packet loss measurement is enabled for all mid-points. If this parameter is not configured, on-demand packet loss measurement is enabled for all measurement points. **NOTE** The mid-point is only applied to hop-by-hop measurement.	-
time-range *time-range*	Specifies the time range for statistics collection.	The value is 5, 10, 15, or 30, in minutes. The default value is 10 minutes.

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

This command is not recorded in the configuration file after being executed.

After device restart, statistics collection based on the time range becomes invalid, and needs to be reconfigured.

Statistics collection based on the time range and continual statistics collection cannot be enabled simultaneously.

Example

Enable statistics collection based on the time range for a measurement instance on a DCP.

```
<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
```

16.5.36 loss-measure enable continual

Function

The **loss-measure enable continual** command enables continual statistics collection for a measurement instance on a DCP.

The **undo loss-measure enable continual** command disables continual statistics collection for a measurement instance on a DCP.

By default, continual statistics collection is disabled for a measurement instance on a DCP.

Format

loss-measure enable continual

undo loss-measure enable continual

Parameters

None

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you are unaware of network performance degrading and want to continuously monitor packet loss on the network, run the **loss-measure enable continual** command to enable continual statistics collection.

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

Continual statistics collection and statistics collection based on the time range cannot be enabled simultaneously.

Example

Enable continual statistics collection for a measurement instance on a DCP.

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

16.5.37 loss-measure ratio-threshold

Function

The **loss-measure ratio-threshold** command configures the alarm and clear alarm thresholds of the packet loss ratio for a measurement instance on the MCP.

The **undo loss-measure ratio-threshold** command restores the default setting.

By default, the alarm and clear alarm thresholds of the packet loss ratio are not configured for a measurement instance on the MCP. That is, no alarm is generated for packet loss.

Format

loss-measure ratio-threshold upper-limit *upper-limit* **lower-limit** *lower-limit*

undo loss-measure ratio-threshold

Parameters

Parameter	Description	Value
upper-limit *upper-limit*	Specifies the alarm threshold for the packet loss ratio.	The value is a string of 1 to 10 digits and in the range of 0.000001 to 100. The value is accurate to six decimal places, in percentage.
lower-limit *lower-limit*	Specifies the clear alarm threshold for the packet loss ratio.	The value is a string of 1 to 10 digits and in the range of 0.000001 to 100. The value is accurate to six decimal places, in percentage. *lower-limit* must be smaller than or equal to *upper-limit*.

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm and clear alarm thresholds of the packet loss ratio are configured for a measurement instance on the MCP:

- If the packet loss ratio in five consecutive measurement intervals exceeds the alarm threshold, the MCP reports the hwIpfpmLossRatioExceed alarm to the NMS to notify the link fault in real time.
- If the packet loss ratio in five consecutive measurement intervals falls below the clear alarm threshold, the MCP reports the hwIpfpmLossRatioRecovery alarm to the NMS to notify link recovery in real time.

To facilitate operation and maintenance, you are advised to run this command to configure the alarm and clear alarm thresholds of the packet loss ratio for a measurement instance on the MCP according to network performance.

Precautions

If you run the **loss-measure ratio-threshold** command multiple times, only the latest configuration takes effect.

This command only configures the alarm and clear alarm thresholds of the packet loss ratio for a measurement instance on the MCP. The hwIpfpmLossRatioExceed and hwIpfpmLossRatioRecovery alarms are triggered only when the alarm and clear alarm functions are enabled and the packet loss ratio in five consecutive measurement intervals reaches the threshold.

Example

Set the alarm and clear alarm thresholds of the packet loss ratio to 10% and 5.5% for measurement instance 1.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] loss-measure ratio-threshold upper-limit 10 lower-limit 5.5
```

16.5.38 mcp (IPFPM-DCP view)

Function

The **mcp** command associates the MCP ID with all measurement instances of a DCP.

The **undo mcp** command disassociates the MCP ID from all measurement instances of a DCP.

By default, no MCP ID is associated with a measurement instance of 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 the MCP ID associated with all measurement instances of a DCP. It is recommended that you configure the router ID of the device as the MCP ID.	The value is in dotted decimal notation.
port *port-number*	Specifies the UDP port number through which the DCP and MCP communicate with each other.	The value is an integer that ranges from 1024 to 65535. The default value is 65030 and is recommended.
vpn-instance *vpn-instance-name*	Specifies the VPN instance where the DCP and MCP communicate with each other.	The value must be an existing VPN instance name.
net-manager-vpn	Specifies the manager VPN where the DCP and MCP communicate with each other.	-

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the IP Flow Performance Measurement (FPM) system, each measurement instance belongs to an MCP. Before a DCP sends statistics data of a measurement instance from TLPs to the MCP, you must associate the MCP ID with the measurement instance. The **mcp** command associates the MCP ID with all measurement instances of a DCP.

A DCP encapsulates statistics data collected from Target Logical Ports (TLPs) and MCP ID associated with all measurement instances on the DCP in a packet, and sends the packet with the MCP ID as the destination IP address. After receiving the packet sent from the DCP, the MCP compares the MCP ID in the packet with the MCP ID configured by the **mcp id** command:

- If the two MCP IDs are the same, the MCP accepts the packet, and then summarizes and calculates the statistics data.
- If the two MCP IDs are different, the MCP considers the packet invalid and discards it.

Prerequisites

Global DCP has been enabled using the **nqa ipfpm dcp** command.

NOTE

If the DCP is required to send statistics data to the MCP through a specified VPN instance or manager VPN, the VPN instance must have been created on the DCP before you run the **mcp** command with **vpn-instance** *vpn-instance-name* or **net-manager-vpn** specified.

Precautions

The MCP ID must be an IP address that DCPs can reach and must be the same as the MCP ID configured by the **mcp id** command on the MCP.

The UDP port number through which the DCP and MCP communicate with each other must be the same as the UDP port number configured by the **protocol udp port** command.

The **mcp** command associates the MCP ID with all measurement instances on the DCP. However, if some measurement instances on the DCP have been associated with the MCP ID configured by the **mcp** command, the measurement instances still use the MCP ID in the IPFPM-DCP instance view.

Example

Associate the MCP ID with all measurement instances of a DCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] mcp 10.1.1.1
```

16.5.39 mcp (IPFPM-DCP instance view)

Function

The **mcp** command associates the MCP ID with a measurement instance of a DCP.

The **undo mcp** command disassociates the MCP ID from a measurement instance of a DCP.

By default, no MCP ID is associated with a measurement instance of 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 the MCP ID associated with a measurement instance of a DCP. It is recommended that you configure the router ID of the device as the MCP ID.	The value is in dotted decimal notation.

Parameter	Description	Value
port *port-number*	Specifies the UDP port number through which the DCP and MCP communicate with each other.	The value is an integer that ranges from 1024 to 65535. The default value 65030 is recommended.
vpn-instance *vpn-instance-name*	Specifies the VPN instance where the DCP and MCP communicate with each other.	The value is a string of 1 to 31 case-sensitive characters without spaces.
net-manager-vpn	Specifies the manager VPN where the DCP and MCP communicate with each other.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before a DCP sends statistics data of a measurement instance from TLPs to the MCP, you must associate the MCP ID with the measurement instance. The **mcp** command associates the MCP ID with a measurement instance of a DCP.

A DCP encapsulates statistics data collected from Target Logical Ports (TLPs) and MCP ID associated with a measurement instance of the DCP in a packet, and sends the packet with the MCP ID as the destination IP address. After receiving the packet sent from the DCP, the MCP compares the MCP ID in the packet with the MCP ID configured by the **mcp id** command:

- If the two MCP IDs are the same, the MCP accepts the packet, and then summarizes and calculates the statistics data.
- If the two MCP IDs are different, the MCP considers the packet invalid and discards it.

Prerequisites

A measurement instance has been created on the DCP using the **instance** command.

Precautions

The MCP ID must be an IP address that DCPs can reach and must be the same as the MCP ID configured by the **mcp id** command on the MCP.

The UDP port number through which the DCP and MCP communicate with each other must be the same as the UDP port number configured by the **protocol udp port** command.

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.

Example

Associate the MCP ID with a measurement instance of 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
```

16.5.40 mcp id

Function

The **mcp id** command configures the MCP ID in the IP Flow Performance Measurement (FPM) system.

The **undo mcp id** command deletes the MCP ID.

By default, no MCP ID is configured.

Format

mcp id *mcp-id*

undo mcp id

Parameters

Parameter	Description	Value
mcp-id	Specifies the MCP ID. It is recommended that you configure the router ID of the device as the MCP ID.	The value is in dotted decimal notation.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the MCP communicates with a DCP, the DCP encapsulates statistics data collected from TLPs and MCP ID associated with a measurement instance by the **mcp** command in a packet, and sends the packet with the MCP ID as the destination IP address. After receiving the packet sent from the DCP, the MCP compares the MCP ID in the packet with the MCP ID of the device:

- If the two MCP IDs are the same, the MCP accepts the packet, and then summarizes and calculates the statistics data.
- If the two MCP IDs are different, the MCP considers the packet invalid and discards it.

This command configures the MCP ID.

Prerequisites

Global MCP has been enabled using the **nqa ipfpm mcp** command.

Precautions

The MCP ID must be an IP address that a DCP can reach and must be the same as the MCP ID configured by the **mcp** command on the DCP. If you have changed the MCP ID, you must change the MCP ID associated with measurement instances on the DCP; otherwise, the DCP cannot communicate with the MCP.

Example

Set the MCP ID.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] mcp id 10.1.1.1
```

16.5.41 measure disable (IPFPM-MCP instance view)

Function

The **measure disable** command disables measurement of all indicators in a measurement instance on the MCP.

Both the **undo measure disable** and **measure enable** commands enable measurement of all indicators in a measurement instance on the MCP.

By default, measurement of all indicators is enabled in a measurement instance on the MCP.

Format

measure disable

measure enable

undo measure disable

Parameters

None

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

If the MCP receives error data during the DCP configuration update, you can run the **measure disable** command to disable measurement of all indicators in a measurement instance on the MCP. When the DCP configuration update is complete, run the **undo measure disable** or **measure enable** command to enable measurement of all indicators in a measurement instance on the MCP so that data of the measurement instance is more accurate.

Example

Disable measurement of all indicators in measurement instance 1 on the MCP.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] measure disable
```

16.5.42 nqa ipfpm dcp

Function

The **nqa ipfpm dcp** command enables global DCP and displays the IPFPM-DCP view, or directly displays the IPFPM-DCP view if global DCP has been enabled.

The **undo nqa ipfpm dcp** command disables global DCP.

By default, global DCP is disabled.

Format

nqa ipfpm dcp

undo nqa ipfpm dcp

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before performing packet loss measurement for service traffic, run the **nqa ipfpm dcp** command to enable global DCP and enter the IPFPM-DCP view.

Follow-up Procedure

Run the **dcp id** command to set the DCP ID.

Precautions

DCP and MCP functions can be configured on the same device.

Example

Enable global DCP and enter the IPFPM-DCP view.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp]
```

16.5.43 nqa ipfpm mcp

Function

The **nqa ipfpm mcp** command enables global MCP and displays the IPFPM-MCP view, or directly displays the IPFPM-MCP view if global MCP has been enabled.

The **undo nqa ipfpm mcp** command disables global MCP.

By default, global MCP is disabled.

Format

nqa ipfpm mcp

undo nqa ipfpm mcp

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before performing packet loss measurement for service traffic, run the **nqa ipfpm mcp** command to enable global MCP and enter the IPFPM-MCP view.

Follow-up Procedure

Run the **mcp id** command to set the MCP ID.

Precautions

MCP and DCP functions can be configured on the same device.

Example

Enable global MCP and enter the IPFPM-MCP view.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp]
```

16.5.44 out-group

Function

The **out-group** command creates a Target Logical Port (TLP) out-group for the target flow.

The **undo out-group** command deletes a TLP out-group or deletes a TLP from a TLP out-group.

By default, no TLP out-group is configured for the target flow.

Format

out-group dcp *dcp-id* **tlp** *tlp-id*

undo out-group [**dcp** *dcp-id* **tlp** *tlp-id*]

Parameters

Parameter	Description	Value
dcp *dcp-id*	Indicates a DCP to which TLPs in a TLP out-group belongs.	This value is in dotted decimal notation.
tlp *tlp-id*	Indicates a TLP in a TLP out-group.	The value is an integer ranging from 1 to 16777215.

Views

IPFPM-MCP-ACH view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To measure the packet loss or delay of service packets leaving a network, run the **out-group** command. In IP FPM hop-by-hop performance statistics scenarios, a

hop is a set of links and interfaces that service packets travel through, from one measurement point or group to the next measurement point or group, and therefore is represented by (TLP in-group, TLP out-group). Performance statistics are implemented on the TLP in-point or in-group through which service packets enter a network and the TLP out-point or out-group through which service packets leave the network.

Prerequisites

The **ach** command has been run to create an ACH and display the ACH view.

Example

Create a TLP out-group for the target flow.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] instance 1
[HUAWEI-nqa-ipfpm-mcp-instance-1] ach 1
[HUAWEI-nqa-ipfpm-mcp-instance-1-ach-1] out-group dcp 10.1.1.1 tlp 100
```

16.5.45 protocol udp port

Function

The **protocol udp port** command configures the UDP port number through which the DCP and MCP communicate with each other.

The **undo protocol udp port** command restores the default UDP port number through which the DCP and MCP communicate with each other.

By default, the DCP and MCP communicate with each other through UDP port 65030. The default configuration is recommended.

Format

protocol udp port *port-number*

undo protocol udp port

Parameters

Parameter	Description	Value
port-number	Specifies the UDP port number through which the DCP and MCP communicate with each other.	The value is an integer that ranges from 1024 to 65535.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DCP uses UDP and default port 65030 to send statistics data to the MCP. To change the UDP port number, run this command.

Prerequisites

Global MCP has been enabled using the **nqa ipfpm mcp** command.

Precautions

The UDP port number of the DCP must be the same as the UDP port number configured by the **mcp (IPFPM-DCP instance view)** command on the DCP. 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.

Example

Specify UDP port 1024 through which the DCP and MCP communicate with each other.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm mcp
[HUAWEI-nqa-ipfpm-mcp] protocol udp port 1024
```

16.5.46 tlp

Function

The **tlp** command configures Target Logical Ports (TLPs) of an IP FPM instance and their roles.

The **undo tlp** command deletes TLPs of a measurement instance.

By default, no TLP of a measurement instance is configured.

Format

tlp *tlp-id* { **in-point** | **out-point** } { **ingress** | **egress** }

tlp *tlp-id* **mid-point flow** { **forward** | **backward** | **bidirectional** } { **ingress** | **egress** }

undo tlp *tlp-id*

Parameters

Parameter	Description	Value
tlp-id	Specifies the ID of a TLP.	The value is an integer that ranges from 1 to 16777215.

Parameter	Description	Value
in-point	Indicates the in-point TLP. An in-point TLP colors a target flow.	-
out-point	Indicates the out-point TLP. An out-point TLP removes the color flag from a target flow.	-
ingress	Indicates the ingress TLP. An ingress TLP only receives packets.	-
egress	Indicates the egress TLP. An egress TLP only sends packets.	-
mid-point	Indicates the TLP as a mid-point.	-
flow	Indicates the target flow.	-
forward	Indicates the forward target flow.	-
backward	Indicates the backward target flow.	-
bidirectional	Indicates the bidirectional target flows.	-

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** command applies only to the forward target flow, and the reverse of the specified role is used for the backward target flow.
- Mid-points apply only to IP FPM hop-by-hop performance statistics scenarios. Therefore, you must configure **flow** to specify the target flow direction when specifying a TLP as a mid-point.

- A TLP cannot function as both the in-point and out-point for the same unidirectional target flow.
- After an in-point is specified, the packets that match corresponding rules are modified for identification and statistics collection. To ensure that user services are not affected, ensure that an out-point is configured on the upstream device to restore user packets.

Example

Configure TLP 100 and its role for measurement instance 1.

```
<HUAWEI> system-view
[HUAWEI] nqa ipfpm dcp
[HUAWEI-nqa-ipfpm-dcp] instance 1
[HUAWEI-nqa-ipfpm-dcp-instance-1] tlp 100 in-point ingress
```

16.6 iPCA 2.0 Configuration Commands

16.6.1 Command Support

All models of S300, S500, S2700, S5700, and S6700 series switches (except the S5731-L and S5731S-L) support iPCA 2.0.

16.6.2 display s-ipfpm configuration

Function

The **display s-ipfpm configuration** command displays the iPCA 2.0 configuration.

Format

display s-ipfpm configuration [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the iPCA 2.0 configuration is complete, you can run this command to check whether the configuration is correct.

Example

Display the iPCA 2.0 configuration (S5732-H is used as an example).

```
<HUAWEI> display s-ipfpm configuration
Global measure interval(s)                : 60(default)
Global measure color-flag                 : Flags-bit0(default)
Report loss reason                        : disable(default)

Total flow(s) of five tuple               : 2
Total flow(s) of application              : 2
Total flow(s) of UCL group                : 1
Total flow(s) of UCL group and application : 1
Total measure interface(s)/VAP(s)         : 5

Five tuple flow list(s):
------------------------------------------------------------------------------
Flow  Protocol  SrcPort      DstPort      SrcIp/Mask          DstIp/Mask
------------------------------------------------------------------------------
10    -         -            -           10.0.0.0/8          20.0.0.0/8
11    UDP       10000-20000  30000       1.0.0.0/8           11.11.11.11/32
------------------------------------------------------------------------------
Total: 2

Application flow list(s):
------------------------------------------------------------------------------
Flow  Application
------------------------------------------------------------------------------
1000  rtp
1002  ftp, tcp, rtp, qq
------------------------------------------------------------------------------
Total: 2

UCL group flow list(s):
------------------------------------------------------------------------------------------------------------------------

Flow  GroupId  GroupName                    Status
------------------------------------------------------------------------------------------------------------------------

777   11       NA                           Active
------------------------------------------------------------------------------------------------------------------------

Total: 1

UCL group and application flow list(s):
------------------------------------------------------------------------------------------------------------------------

Flow  GroupId  GroupName                    Status    Application
------------------------------------------------------------------------------------------------------------------------
666   11       NA                           Active    UD_DDP
------------------------------------------------------------------------------------------------------------------------

Total: 1

Measure list(s):
I: In-Point,  O: Out-Point, M: Mid-Point
ING: Ingress, EGR: Egress,  B: Bidirectional
------------------------------------------------------------------------------
Interface/VAPProfileName            Flow  AutoDetect  Direction
------------------------------------------------------------------------------
GigabitEthernet0/0/10               10    -           I/ING/B
GigabitEthernet0/0/11               -     YES         M/EGR/B
GigabitEthernet0/0/12               11    -           O/ING/B
test                                10    -           I/ING/B
```



```
test1                          11   -         I/ING/B
------------------------------------------------------------------------------
Total: 5
```

Table 16-57 Description of the **display s-ipfpm configuration** command output

Item	Description
Global measure interval(s)	Packet loss and delay measurement interval. To configure this parameter, run the **s-ipfpm measure interval** command.
Global measure color-flag	Color bit for packet loss and delay measurement. To configure this parameter, run the **s-ipfpm measure color-flag** command.
Report loss reason	Whether the device reports the packet loss cause to the analyzer. To configure this parameter, run the **s-ipfpm report-loss-reason enable** command.
Total flow(s) of five tuple	Number of measurement flow tables based on 5-tuple.
Total flow(s) of application	Number of measurement flow tables based on applications.
Total flow(s) of UCL group	Number of measurement flow tables based on UCL groups.
Total flow(s) of UCL group and application	Number of measurement flow tables based on UCL groups and applications.
Total measure interface(s)/VAP(s)	Number of interfaces and VAP profiles enabled with packet loss and delay measurement.
Five tuple flow list(s)	5-tuple information of the measurement flow. To configure this parameter, run the **s-ipfpm flow** command.
Flow	Measurement flow ID.
Protocol	Protocol type of the measurement flow.
SrcPort	Source port number of the measurement flow.
DstPort	Destination port number of the measurement flow.
SrcIp/Mask	Source IP address of the measurement flow.
DstIp/Mask	Destination IP address of the measurement flow.

Item	Description
Total	Total number of measurement flows.
Application flow list(s)	Information about measurement flows based on applications. To configure this parameter, run the **s-ipfpm flow application** command.
Application	Application name.
UCL group flow list(s)	Information about measurement flows based on UCL groups. To configure this parameter, run the **s-ipfpm flow source-ucl-group** command.
UCL group and application flow list(s)	Information about measurement flows based on UCL groups and applications. To configure this parameter, run the **s-ipfpm flow source-ucl-group** command.
GroupId	UCL group ID.
GroupName	UCL group name. If no UCL group is configured, **NA** is displayed.
Status	Whether a UCL group has been created. To create a UCL group, run the **ucl-group (system view)** command. ● Active: The UCL group has been created. ● Inactive: The UCL group has not been created.
Interface/VAPProfileName	Name of the interface on which packet loss and delay measurement is enabled using the **s-ipfpm measure flow** (interface view) command and name of the VAP profile in which packet loss and delay measurement is enabled using the **s-ipfpm measure flow** (VAP profile view) command.
Flow	Measurement flow ID.
AutoDetect	Whether automatic in-band flow measurement is enabled on an interface. To configure this function, run the **s-ipfpm measure auto-detect** command.
Direction	Measurement point and measurement direction.

16.6.3 s-ipfpm clear color-flag ingress

Function

The **s-ipfpm clear color-flag ingress** command enables the function of clearing the packet color bit in the ingress direction of an interface.

The **undo s-ipfpm clear color-flag ingress** command disables the function of clearing the packet color bit in the ingress direction of an interface.

By default, the function of clearing the packet color bit in the ingress direction of an interface is disabled on the device.

NOTE

This command is supported only by the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

This command can be configured in the VAP profile view only on the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H.

Format

s-ipfpm clear color-flag ingress

undo s-ipfpm clear color-flag ingress

Parameters

None

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view, VAP profile view

Default Level

2: Configuration level

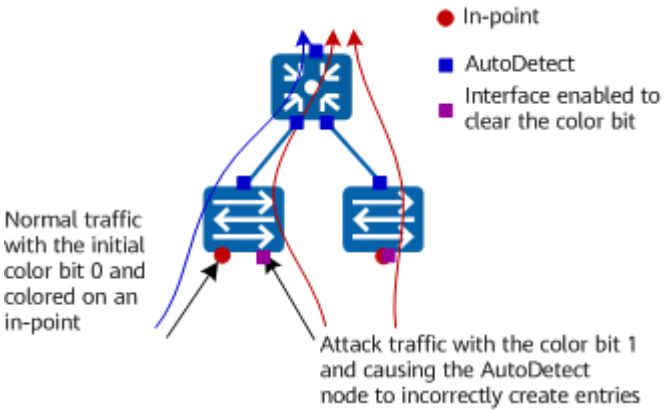
Usage Guidelines

After automatic in-band flow measurement is configured on a downstream device, the downstream device automatically creates a measurement entry and performs measurement for the packets with color bit 1. When an attack occurs on the network (the color bit of attack packets is set to 1) or the color bit of other service packets on the upstream device is set to 1, the measurement data on the downstream device is incorrect. In this case, you can run this command on the inbound interface of packets on the upstream device to enable the function of clearing the packet color bit in the ingress direction. After this function is enabled, the color bit in incoming packets is set to 0, and measurement is not performed for the packets after they are forwarded to the downstream device.

In **Figure 16-1**, on the left device, the interface that receives attack traffic is different from the interface configured as an in-point. The attack traffic is

forwarded to the downstream AutoDetect node based on a forwarding entry. In this case, you need to enable the function of clearing the packet color bit in the ingress direction of the inbound interface that receives the attack traffic on the upstream device. On the right device, the interface that receives attack traffic is the same as the interface configured as an in-point. You need to enable the function of clearing the packet color bit in the ingress direction on this interface. In this way, normal traffic is colored on the in-point, and attack traffic is not colored, ensuring that the downstream device performs measurement only for normal traffic.

Figure 16-1 Attack traffic processing



Example

Enable the function of clearing the packet color bit in the ingress direction of GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] s-ipfpm clear color-flag ingress
```

16.6.4 s-ipfpm flow

Function

The **s-ipfpm flow** command configures a measurement flow.

The **undo s-ipfpm flow** command deletes a configured measurement flow.

By default, no measurement flow is configured.

Format

s-ipfpm flow *flow-id* { **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* } } *

undo s-ipfpm flow *flow-id*

Parameters

Parameter	Description	Value
flow-id	Specifies the ID of a measurement flow.	The value is an integer in the range from 0 to 1023. When a measurement flow is specified by application name, the value is in the range from 512 to 1023.
source *src-ip-address*	Specifies the source IP address of a measurement flow. The value can only be a unicast IP address.	The value is in dotted decimal notation.
src-mask-length	Specifies the mask length of the source IP address of a measurement flow.	The value is an integer in the range from 1 to 32.
destination *dest-ip-address*	Specifies the destination IP address of a measurement flow. The value can only be a unicast IP address.	The value is in dotted decimal notation.
dest-mask-length	Specifies the mask length of the destination IP address of a measurement flow.	The value is an integer in the range from 1 to 32.
protocol { **tcp** | **udp** }	Indicates that the protocol type of a measurement flow is TCP or UDP.	-
source-port *src-port-number1*	Specifies the start source port number of a measurement flow.	The value is an integer in the range from 1 to 65535.
src-port-number2	Specifies the end source port number of a measurement flow.	The value is an integer in the range from 1 to 65535. The value of *src-port-number2* must be greater than that of *src-port-number1*.
destination-port *dest-port-number1*	Specifies the start destination port number of a measurement flow.	The value is an integer in the range from 1 to 65535.

Parameter	Description	Value
dest-port-number2	Specifies the end destination port number of a measurement flow.	The value is an integer in the range from 1 to 65535. The value of *dest-port-number2* must be greater than that of *dest-port-number1*.
protocol-number	Specifies a protocol number for a measurement flow.	The value is an integer in the range from 1 to 5, 7 to 16, or 18 to 255. The values 6 and 17 indicate TCP and UDP, respectively.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When delay occurs during traffic transmission or you want to monitor network transmission quality in real time, you can configure iPCA 2.0 on devices to monitor network performance. A measurement flow is a key element for configuring iPCA 2.0. Before each measurement, you must configure a measurement flow.

A measurement flow can be defined by any combinations of the source IP address, destination IP address, protocol type, source port number, and destination port number. The device generates accurate 5-tuple matching rules for measurement based on the configured parameters.

Precautions

- All devices on a network must have the same measurement flow configuration.
- If a measurement flow is used by an interface, it cannot be deleted.
- WLAN services can use only measurement flows with IDs 0 to 127. Therefore, if WLAN services are configured on a network, you are advised not to use measurement flows with IDs 0 to 127 for other services.
- The source and destination port numbers of a measurement flow cannot be both configured as port number ranges.
- The source IP address/mask length and destination IP address/mask length of a measurement flow cannot be the same.

Example

Configure a measurement flow with the source port number 3, destination port number 10, source IP address 1.1.1.1/24, destination IP address 2.2.2.2/24, and protocol type TCP for packet loss and delay measurement.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm flow 2 protocol tcp source-port 3 destination-port 10 source 1.1.1.1 24 destination 2.2.2.2 24
```

16.6.5 s-ipfpm flow application

Function

The **s-ipfpm flow application** command configures a measurement flow based on an application name.

The **undo s-ipfpm flow** command deletes a measurement flow configured based on an application name.

By default, a measurement flow based on an application name is not configured on the device.

NOTE

This command is supported only by the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

s-ipfpm flow *flow-id* **application** { *app-name* } &<1-16>

undo s-ipfpm flow *flow-id*

Parameters

Parameter	Description	Value
flow-id	Specifies the ID of a measurement flow.	The value is an integer in the range from 512 to 1023.
application *app-name*	Specifies the application name corresponding to a measurement flow.	The value is a string of 1 to 64 case-insensitive characters. If the application name contains spaces, it must be enclosed in double quotation marks, for example, "user for test". A maximum of 16 application names can be configured at a time, and multiple application names configured at a time can be the same.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When delay occurs during traffic transmission or you want to monitor network transmission quality in real time, you can configure iPCA 2.0 on devices to monitor network performance. A measurement flow is a key element for configuring iPCA 2.0. Before each measurement, you must configure a measurement flow.

A measurement flow can be specified based on an application name so that the device performs measurement for traffic of the application.

Precautions

- All devices on a network must have the same measurement flow configuration.
- If a measurement flow is used by an interface, the measurement flow cannot be deleted.

Follow-up Procedure

Run the **s-ipfpm measure flow** command to enable traffic measurement in the interface view.

Example

Configure the device to perform measurement for packets of the application named **QQLive**.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm flow 533 application QQLive
```

16.6.6 s-ipfpm flow source-ucl-group

Function

The **s-ipfpm flow source-ucl-group** command configures a measurement flow based on a UCL group or a UCL group and an application.

The **undo s-ipfpm flow** command deletes a measurement flow configured based on a UCL group or a UCL group and an application.

By default, a measurement flow based on a UCL group or a UCL group and an application is not configured on the device.

NOTE

This command is supported only by the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

s-ipfpm flow *flow-id* **source-ucl-group** { *group-index* | **name** *group-name* } &<1-16>

s-ipfpm flow *flow-id* **application** { *app-name* } &<1-16> **source-ucl-group** { *group-index* | **name** *group-name* }

undo s-ipfpm flow *flow-id*

Parameters

Parameter	Description	Value
flow-id	Specifies the ID of a measurement flow.	The value is an integer in the range from 512 to 1023.
group-index	Specifies the index of a source UCL group.	The value is an integer in the range from 1 to 64000.
name *group-name*	Specifies the name of a source UCL group.	The value must be the name of an existing UCL group. A maximum of 16 UCL group indexes and UCL group names can be configured at a time, and multiple UCL group indexes and UCL group names configured at a time can be the same.
application *app-name*	Specifies the name of an application.	The value is a string of 1 to 64 case-insensitive characters. If the application name contains spaces, it must be enclosed in double quotation marks, for example, "user for test". A maximum of 16 application names can be configured at a time, and multiple application names configured at a time can be the same.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When delay occurs during traffic transmission or you want to monitor network transmission quality in real time, you can configure iPCA 2.0 on devices to monitor

network performance. A measurement flow is a key element for configuring iPCA 2.0. Before each measurement, you must configure a measurement flow.

A measurement flow can be specified based on a UCL group or a UCL group and an application so that the device performs measurement for traffic of all users in the UCL group.

Precautions

- All devices on a network must have the same measurement flow configuration.
- If a measurement flow is used by an interface, the measurement flow cannot be deleted.
- If a UCL group index is not created, this command can be configured when the UCL group index is specified. If a UCL group name is not configured, this command cannot be configured when the UCL group name is specified. After a UCL group name is configured in a measurement flow, the UCL group name cannot be deleted.

Follow-up Procedure

Run the **s-ipfpm measure flow** command to enable traffic measurement in the interface view.

Example

Configure the device to perform measurement for packets of users in the UCL group with index 10.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm flow 533 source-ucl-group 10
```

16.6.7 s-ipfpm measure application

Function

The **s-ipfpm measure application** command enables packet loss and delay measurement based on the application name in the VAP profile view.

The **undo s-ipfpm measure application** command disables packet loss and delay measurement based on the application name in the VAP profile view.

By default, packet loss and delay measurement based on the application name is disabled in the VAP profile view.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H support this command.

Format

s-ipfpm measure application { *app-name* } &<1-16>

undo s-ipfpm measure application { *app-name* } &<1-16>

Parameters

Parameter	Description	Value
application *app-name*	Specifies the name of an application for which packet loss and delay measurement is performed.	The application name must exist in the application signature database. A maximum of 16 application names can be configured at a time.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an application on a wireless network has poor user experience (for example, video freezing or voice discontinuity) or you want to monitor the network transmission quality of an application in real time, you can enable packet loss and delay measurement for the application on the switch.

Precautions

- Before configuring this command, you must run the **defence engine enable ap-group** { **all** | **name** *ap-group-name* } command to enable the security engine function for an AP group.
- This command cannot be configured after the **s-ipfpm measure flow** command is run in the VAP profile view to enable packet loss and delay measurement.
- After the **s-ipfpm measure application** command is configured to enable packet loss and delay measurement based on an application name in the VAP profile view, user packets corresponding to the application name will be modified for identification and statistics collection. To ensure that user services are not affected, ensure that an out-point is configured on the upstream device to restore user packets.

Example

Configure packet loss and delay measurement for the application named **baidu**.

```
<HUAWEI> system-view
[HUAWEI] defence engine enable ap-group name test
Info: Make sure the group name of AP exists. Continue? [Y/N]:y
It will take several minutes to load the signature lib, please wait....
Info: The signature lib load successful.
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name test
[HUAWEI-wlan-vap-prof-test] s-ipfpm measure application baidu
```


16.6.8 s-ipfpm measure color-flag

Function

The **s-ipfpm flow** command configures a color bit for packet loss and delay measurement.

The **undo s-ipfpm measure color-flag** command restores the default color bit for packet loss and delay measurement.

By default, bit 0 in the Flags field of the IP header is used as the color bit for packet loss and delay measurement on the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, and bit 5 in the ToS field of the IP header is used as the color bit for packet loss and delay measurement on other models.

Format

s-ipfpm measure color-flag { **tos-bit** *tos-bit* | **flags-bit0** }

undo s-ipfpm measure color-flag

Parameters

Parameter	Description	Value
tos-bit *tos-bit*	Specifies a bit in the ToS field of the IP header as the color bit for packet loss and delay measurement.	The value is an integer in the range from 3 to 7 for the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S and in the range from 3 to 5 for other models.
flags-bit0	Specifies bit 0 in the Flags field of the IP header as the color bit for packet loss and delay measurement.	This parameter is supported only by the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When delay occurs during traffic transmission or you want to monitor network transmission quality in real time, you can configure iPCA 2.0 on devices to monitor

network performance. You can run this command to specify the color bit for packet loss and delay measurement. You can select a proper color bit based on your requirements and network planning.

Precautions

- All devices on a network must use the same color bit setting.
- When the DS field is used to provide differentiated services for QoS, it is not recommended that you configure bits 3 to 5 in the ToS field as color bits because the packet loss and delay measurement result may be inaccurate.
- When bits 3 to 5 in the ToS field are used as color bits, you must run the **dynamic flow inspection disable** command in the VAP profile view to disable the Deep Flow Inspection (DFI) function on a VAP. Otherwise, the measurement function is abnormal because the DFI function on a VAP will decolor color bits 3 to 5 in the ToS field.
- If the Explicit Congestion Notification (ECN) function is configured on a device on the network, bits 6 and 7 in the ToS field cannot be used as color bits because the ECN function uses these two bits. If they are used as color bits, a switch sends packets with the color bits to a downstream device, affecting the ECN function.

Example

Configure bit 3 in the ToS field as the color bit for packet loss and delay measurement.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm measure color-flag tos-bit 3
```

16.6.9 s-ipfpm measure interval

Function

The **s-ipfpm measure interval** command configures the packet loss and delay measurement interval.

The **undo s-ipfpm measure interval** command restores the default packet loss and delay measurement interval.

By default, the packet loss and delay measurement interval is 60 seconds.

Format

s-ipfpm measure interval *interval*

undo s-ipfpm measure interval

Parameters

Parameter	Description	Value
interval	Specifies the packet loss and delay measurement interval.	The value can be 10 or 60, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packet loss or delay occurs during traffic transmission or you want to monitor network transmission quality in real time, you can configure iPCA 2.0 on devices to monitor network performance. You can run this command to specify the packet loss and delay measurement interval on a device.

Precautions

- The measurement interval must be the same on all devices configured with measurement flows. Otherwise, there is no measurement data.
- The measurement interval cannot be changed during measurement. To change the measurement interval, you are advised to disable the measurement flows bound to all interfaces first. Otherwise, the packet loss and delay data calculated in subsequent measurement intervals may be incorrect.
- On a large network, changing the measurement interval to 10 seconds affects the measurement performance. Therefore, exercise caution when changing the measurement interval.

Example

Set the packet loss and delay measurement interval to 60 seconds.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm measure interval 60
```

16.6.10 s-ipfpm measure auto-detect

Function

The **s-ipfpm measure auto-detect** command enables automatic in-band flow measurement on an interface.

The **undo s-ipfpm measure auto-detect** command disables automatic in-band flow measurement on an interface.

By default, automatic in-band flow measurement is disabled on an interface.

NOTE

This command is supported only by the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

s-ipfpm measure auto-detect { **out-point** | **mid-point** } { **ingress** | **egress** } [**bidirectional**]

undo s-ipfpm measure auto-detect

Parameters

Parameter	Description	Value
out-point	Indicates that a measurement point for automatic in-band flow measurement is an out-point. An out-point removes the color bit from a measurement flow.	-
mid-point	Indicates that a measurement point for automatic in-band flow measurement is a mid-point.	-
ingress	Indicates that measurement is performed in the ingress direction. On this measurement point, the system measures the packets received by the interface.	-
egress	Indicates that measurement is performed in the egress direction. On this measurement point, the system measures the packets sent by the interface.	-
bidirectional	Indicates that measurement is performed in both the ingress and egress directions. When this parameter is specified, a backward flow configuration is added based on reversal of the measurement flow information and measurement direction.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packet loss and delay measurement is performed for a specified flow or application, measurement needs to be performed on all devices on the forwarding path. In this case, you need to specify the 5-tuple information or application name of the flow on all devices. If a large number of flows or applications need to be

measured, the configuration workload is heavy. To simplify the configuration, you can specify the 5-tuple or application name of the flow only on the in-point node and enable automatic in-band flow measurement on the mid-point and out-point nodes. After automatic in-band flow measurement is enabled on the mid-point and out-point nodes, the devices automatically create measurement entries based on the packet coloring on the in-point node to perform traffic measurement.

Precautions

- When automatic in-band flow measurement is configured, if the resource allocation mode is not **enhanced-sipfpm**, measurement flows occupy ACL resources, and the number of measurement flows is limited by the number of ACL resources on the device. When the **enhanced-sipfpm** mode is configured, measurement flows do not occupy ACL resources, which meets the requirements in scenarios where a large number of measurement flows are configured.
- This command can be run on a Layer 2 or Layer 3 interface, but not on a stack interface.

Example

Configure GE0/0/1 as a mid-point to perform automatic in-band flow measurement in the ingress direction.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] s-ipfpm measure auto-detect mid-point ingress
```

16.6.11 s-ipfpm measure flow (interface view)

Function

The **s-ipfpm measure flow** command enables packet loss and delay measurement on an interface.

The **undo s-ipfpm measure flow** command disables packet loss and delay measurement from an interface.

By default, packet loss and delay measurement is disabled on an interface.

Format

s-ipfpm measure flow *flow-id* { **in-point** | **out-point** | **mid-point** } { **ingress** | **egress** } [**bidirectional**]

undo s-ipfpm measure flow *flow-id*

Parameters

Parameter	Description	Value
flow-id	Specifies the ID of a measurement flow.	The value is an integer in the range from 0 to 1023.
in-point	Indicates that a measurement point is an in-point. An in-point colors a measurement flow.	-
out-point	Indicates that a measurement point is an out-point. An out-point removes the color bit from a measurement flow.	-
mid-point	Indicates that a measurement point is a mid-point.	-
ingress	Indicates that measurement is performed in the ingress direction. On this measurement point, the system measures the packets received by the interface.	-
egress	Indicates that measurement is performed in the egress direction. On this measurement point, the system measures the packets sent by the interface.	-
bidirectional	Indicates that measurement is performed in both the ingress and egress directions. When this parameter is specified, a backward flow configuration is added based on reversal of the measurement flow information and measurement direction.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor network transmission quality in real time to quickly detect abnormal traffic and locate faults, you can enable packet loss and delay measurement on interfaces of devices.

Precautions

- Measurement can be performed only for incoming traffic on interfaces for the S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S,S2730S-S, S5735-L-I, S5735-L1, S300, S5735-L, S5735S-L1, S5735S-L, S5735S-L-M, S500, S5735-S, S5735-S-I, S5735S-S ,S6735-S, S6720-EI, S6720S-S, and S6720S-EI.
- This command can be run on a Layer 2 or Layer 3 interface, but not on a stack interface.
- The 5-tuple ranges of multiple measurement flows bound to the same interface cannot overlap.
- Measurement is performed for tunnel packets based on the inner 5-tuple of the packets.
- If the **s-ipfpm flow source-ucl-group** command has been run to configure a measurement flow based on a UCL group or based on a UCL group and application, you can only specify the **in-point** and **ingress** parameters when you run the **s-ipfpm measure flow** command to enable packet loss and delay measurement on an interface.
- After an interface is configured as an in-point using the **s-ipfpm measure flow** *flow-id* **in-point** { **ingress** | **egress** } [**bidirectional**] command, the packets that arrive at the interface and match corresponding rules are modified for identification and statistics collection. To ensure that user services are not affected, ensure that an out-point is configured on the upstream device to restore user packets.

Example

Configure GE0/0/1 as an in-point and enable packet loss and delay measurement in its ingress direction.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm flow 33 protocol tcp source-port 3 destination-port 10 source 1.1.1.1 24 destination 2.2.2.2 24
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] s-ipfpm measure flow 33 in-point ingress
```

16.6.12 s-ipfpm measure flow (VAP profile view)

Function

The **s-ipfpm measure flow** command enables packet loss and delay measurement in the VAP profile view.

The **undo s-ipfpm measure flow** command disables packet loss and delay measurement in the VAP profile view.

By default, packet loss and delay measurement is disabled in the VAP profile view.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H support this command.

Format

s-ipfpm measure flow *flow-id* { **in-point** | **out-point** | **mid-point** } { **ingress** | **egress** } [**bidirectional**]

undo s-ipfpm measure flow *flow-id*

Parameters

Parameter	Description	Value
flow-id	Specifies the ID of a measurement flow.	The value is an integer in the range from 0 to 127.
in-point	Indicates that a measurement point is an in-point. An in-point colors a measurement flow.	-
out-point	Indicates that a measurement point is an out-point. An out-point removes the color bit from a measurement flow.	-
mid-point	Indicates that a measurement point is a mid-point.	-
ingress	Indicates the ingress direction of a measurement flow. On this measurement point, the system measures the packets received by the AP.	-
egress	Indicates the egress direction of a measurement flow. On this measurement point, the system measures the packets sent by the AP.	-
bidirectional	Indicates that a measurement flow is a bidirectional flow. When this parameter is specified, a backward flow configuration is added based on reversal of the 5-tuple and measurement direction.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor wireless network transmission quality in real time in a native AC scenario to quickly detect abnormal traffic and locate faults, you can enable packet loss and delay measurement in the VAP profile view.

Precautions

- A maximum of 64 measurement flows can be bound to a VAP profile.
- The 5-tuple ranges of multiple measurement flows bound to the same VAP profile cannot overlap.
- Measurement is performed for tunnel packets based on the inner 5-tuple of the packets.
- After an in-point is specified using the **s-ipfpm measure flow** *flow-id* **in-point** { **ingress** | **egress** } [**bidirectional**] command, the packets that match corresponding rules are modified for identification and statistics collection. To ensure that user services are not affected, ensure that an out-point is configured on the upstream device to restore user packets.

Example

Enable packet loss and delay measurement in the VAP profile view.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm flow 1 protocol tcp destination-port 5
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name test
[HUAWEI-vap-prof-test] s-ipfpm measure flow 1 in-point ingress
```

16.6.13 s-ipfpm measure max-user-flow

Function

The **s-ipfpm measure max-user-flow** command sets the maximum number of iPCA 2.0 measurement flows for each user.

The **undo s-ipfpm measure max-user-flow** command restores the default maximum number of iPCA 2.0 measurement flows for each user.

By default, the maximum number of iPCA 2.0 measurement flows for each user is not limited but depends on device specifications.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H support this command.

Format

s-ipfpm measure max-user-flow *limit-number*

undo s-ipfpm measure max-user-flow

Parameters

Parameter	Description	Value
limit-number	Specifies the maximum number of iPCA 2.0 measurement flows for each user.	The value is an integer that ranges from 100 to 400.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent a single user from occupying excessive iPCA 2.0 flow entries, you can run this command to set the maximum number of iPCA 2.0 measurement flows for each user.

Example

Set the maximum number of iPCA 2.0 measurement flows for each user to 100.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name apsys
[HUAWEI-wlan-ap-system-prof-apsys] s-ipfpm measure max-user-flow 100
```

16.6.14 s-ipfpm measure ucl-group

Function

The **s-ipfpm measure ucl-group** command specifies a UCL group or a "UCL group + application" combination for iPCA 2.0 measurement.

The **undo s-ipfpm measure ucl-group** command deletes a UCL group or a "UCL group + application" combination for iPCA 2.0 measurement.

By default, iPCA 2.0 measurement is not specified for any UCL group on a VAP.

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6730S-H and S6730-H support this command.

Format

s-ipfpm measure ucl-group { *group-index* | **name** *group-name* } [**application** *application-name* & <1-16>]

undo s-ipfpm measure ucl-group { *group-index* | **name** *group-name* } [**application** *application-name* & <1-16>]

Parameters

Parameter	Description	Value
group-index	Specifies the index of a UCL group.	The value is an integer that ranges from 1 to 64000.
name *group-name*	Specifies the name of a UCL group.	The UCL group must exist.
application *application-name*	Specifies an application for which iPCA 2.0 measurement is performed.	The application name must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To perform UCL group–based iPCA 2.0 measurement based on a VAP, run this command to specify a UCL group or a "UCL group + application" combination on the VAP.

You can specify a UCL group so that the device can perform iPCA 2.0 measurement for applications of users in the specified UCL group. You can also specify a "UCL group + application" combination, so that the device can perform iPCA 2.0 measurement for the specified application of users in the specified UCL group.

Precautions

A maximum of 128 applications, UCL groups, and "UCL group + application" combinations (including 16 applications at most) can be specified for iPCA 2.0 measurement.

If the parameter **application** *application-name* is specified, you need to enable the security engine function (using the **defence engine enable ap-group** { **all** | **name** *ap-group-name* } command) for the AP group.

Example

Specify a "UCL group + application" combination for iPCA 2.0 measurement in the VAP profile view.

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap-profile1
[HUAWEI-wlan-vap-prof-vap-profile1] s-ipfpm measure ucl-group 1 application welink
```

16.6.15 s-ipfpm report-loss-reason enable

Function

The **s-ipfpm report-loss-reason enable** command enables the device to report the packet loss cause to the analyzer.

The **undo s-ipfpm report-loss-reason enable** command disables the device from reporting the packet loss cause to the analyzer.

By default, the device is disabled from reporting the packet loss cause to the analyzer.

NOTE

This command is supported only by the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.

Format

s-ipfpm report-loss-reason enable

undo s-ipfpm report-loss-reason enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

iPCA 2.0 enables devices to report flow measurement information to the analyzer. The analyzer can determine the number of packets discarded on each device for fault locating. However, the packet loss cause cannot be obtained, and maintenance personnel need to manually locate the cause. To address this issue, you can run this command to enable the device to report the packet loss cause to the analyzer. When detecting that packet loss occurs, the device automatically reports the number of lost packets, number of lost bytes, and last packet loss

cause in a period to the analyzer. The analyzer directly displays the packet loss cause, helping maintenance personnel quickly locate faults.

Example

Enable the device to report the packet loss cause to the analyzer.

```
<HUAWEI> system-view
[HUAWEI] s-ipfpm report-loss-reason enable
```

16.7 NQA Configuration Commands

16.7.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.7.2 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.

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
```

16.7.3 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

Usage Scenario

After each test instance is complete, test results and historical information will be recorded in result and historical tables respectively. You can run the following commands to view the corresponding data and assess the network quality.

- The **display nqa results** command displays the results of an NQA test instance.
- The **display nqa history** command displays the historical records of an NQA test instance.

After several test instances are performed to detect network quality, there may be too many records in the statistics table. In this case, you can run the **clear-records** command to clear historical records and result records of an NQA test instance.

Configuration Impact

Statistics cannot be restored after being cleared using the **clear-records** command.

Precautions

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
```

16.7.4 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.

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
[HUAWEI-nqa-user-test1] test-type snmp
[HUAWEI-nqa-user-test1] community read cipher Tester-123
```

16.7.5 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
- UDP Jitter
- ICMP
- Trace
- Path Jitter
- Path MTU

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
```

16.7.6 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

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** Only for MAC ping test instance, the value ranges from 95 to 9000, 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 LSP Ping, LSP Jitter, PWE3 Ping, ICMP, MAC Ping, Path Jitter, Trace, UDP, and UDP Jitter test instances.

Precautions

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
```

16.7.7 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

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
```

16.7.8 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**]

destination-address ipv6 *ipv6-address*

destination-address mac *mac-address*

destination-address remote-mep mep-id *rmep-id*

destination-address url *urlstring*

undo destination-address

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.	-

Parameter	Description	Value
vpn-frr-path	Indicates that the connectivity of the backup VPN FRR LSP will be checked.	-
mac *mac-address*	Specifies a unicast MAC address.	The value is a 12-digit hexadecimal number, in the format of H-H-H. Each H is 4 digits.
remote-mep mep-id *rmep-id*	Specifies the ID of a remote MEP.	The value is an integer that ranges from 1 to 8191.
ipv6 *ipv6-address*	Specifies an IPv6 destination address.	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.
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.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NQA detects service features by creating test instances. In NQA, two test ends are called an NQA client and an NQA server. An NQA test is initiated by the NQA client. For a test instance, the server is specified using the destination IP address configured with the **destination-address** command.

For example, to detect whether the peer device is reachable, run the **nqa** command to create an NQA test instance, set the test type to ICMP, and then run the **destination-address** command to configure the IP address of the peer device as the destination IP address. After that, you can start the test instance. Based on the response packet, you can know whether the peer device is reachable.

Precautions

- The Label Switched Path (LSP) parameters can be configured only for the LSP test instances.
- The **mac** and **remote-mep mep-id** parameters can be configured only for MAC ping test instances.
- Only the destination addresses of HTTP, trace, and DNS test instances can be URL addresses. For the HTTP test instances, only absolute URL addresses are supported.
- The destination addresses of DNS test instances cannot be IPv4 addresses, and the destination URL addresses must contain dots (.); otherwise, the test will fail.
- When a URL is specified as the destination address of an NQA test instance, the NQA test instance cannot be bound to a VPN instance. Otherwise, the test fails.
- 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
```

16.7.9 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.

The default port numbers for test instances of different types are as follows:

- TCP and UDP: 7
- HTTP: 80
- FTP: 21
- Trace: 33434
- Jitter: No default value is available, and the destination port number must be configured.

NOTE

A port number larger than 10000 is recommended for a jitter test instance. A small port number may be conflict with the default port number of a protocol, causing a test failure.

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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NQA detects service features by creating test instances. In NQA, two test ends are called an NQA client and an NQA server. An NQA test is initiated by the NQA client. After test instances are configured with commands on the client, NQA places different types of test instances into various test queues. After the test starts, a response packet is returned. Carriers can then know the operating status about protocols by analyzing the received response packet.

For a test instance, the port for accessing the server is specified using the destination port number configured with the **destination-port** command on the client.

For example, to detect whether the TCP service runs normally on the peer device using a TCP test instance, perform the following configurations:

- On the server: Configure the TCP server used for NQA tests, including the supported client IP address and the TCP port number opened to the client.
- On the client:
  - Create an NQA test instance and set its type to TCP.
  - Configure the IP address of the server as the destination IP address and configure the opened TCP port number on the server as the destination port number.
  - Start the test instance.

Precautions

In the case of a TCP test instance and a UDP test instance, the configured destination port number must be the same as the opened port number on the server.

This command applies to only the FTP, HTTP, TCP, Trace, UDP, and UDP Jitter test instances.

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
```

16.7.10 discovery-pmtu-max

Function

Using the **discovery-pmtu-max** command, you can specify the maximum value for the range of a path MTU test.

Using the **undo discovery-pmtu-max** command, you can restore the default maximum value for the range of a path MTU test.

By default, the maximum value for the range of a path MTU test is 1500 bytes.

Format

discovery-pmtu-max *pmtu-max*

undo discovery-pmtu-max

Parameters

Parameter	Description	Value
pmtu-max	Specifies the maximum value for the range of a path MTU test.	It is an integer ranging from 48 to 9198, in bytes.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **discovery-pmtu-max** command is available only in the path MTU test.

Precautions

For the running test instance, the **discovery-pmtu-max** command cannot be used to change the range of the MTU test.

Example

The maximum value for the range of a specified path MTU test is 1800 bytes.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type pathmtu
[HUAWEI-nqa-user-test] discovery-pmtu-max 1800
```

16.7.11 display nqa history

Function

The **display nqa history** command displays the history records about an NQA test.

Format

display nqa history [**test-instance** *admin-name test-name*]

Parameters

Parameter	Description	Value
test-instance	Indicates NQA test instances.	-
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.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

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 UDP Jitter test instances exists.

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, rtp) 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  success       10.2.1.2      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          UnKnown       2012-07-15 11:16:39.915
 2      1/1/2     0ms     busy          UnKnown       2012-07-15 11:16:39.978
 3      1/1/3     0ms     busy          UnKnown       2012-07-15 11:16:39.40
```

Table 16-58 Description of the **display nqa history** command output

Item	Description
NQA entry(admin, rtp) history	The history records about an NQA test instance: • admin: administrator of an NQA test instance. • rtp: name of an NQA test instance. You can run the **nqa** command to configure this parameter.
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.
Response	Period from the time when a probe packet is sent to the time when a response packet is received.

Item	Description
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.

16.7.12 display nqa results

Function

The **display nqa results** command displays NQA test results.

Format

display nqa results [**test-instance** *admin-name test-name*] [**verbose**]

Parameters

Parameter	Description	Value
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. **NOTE** Only ICMP, UDP, ICMP Jitter, Path MTU, and UDP Jitter test instances support the query of details.	-

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 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.

Precautions

The **display nqa results** command only displays the result of a test instance that has been completed.

When NQA test result table and historical table are displayed in a split screen, latest results are displayed to improve user experience.

By default, the unit of the delay statistics field in the result table is millisecond. The **timestamp-unit** command specifies the unit of delay statistics fields in result tables of the UDP Jitter and ICMP Jitter test instances.

When you run the **display nqa results** command to check the results of a single UDP 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.

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 %
```

Display detailed results of an NQA ICMP test.

```
<HUAWEI> display nqa results test-instance admin icmp verbose
  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 %
   Detailed result information:
```

Table 16-59 Description of the **display nqa results test-instance admin icmp** and **display nqa results test-instance admin icmp verbose** 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. You can run the **nqa** command to configure this parameter.
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. You can run the **test-type** command to configure this parameter.
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.

Item	Description
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, so no test result is obtained or no test result is obtained after the test. • failed: indicates that the test 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.
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. You can run the **destination-address** command to configure this parameter.
Min/Max/Average Completion Time	Minimum/Maximum/Average time taken to complete the test.
Sum/Square-Sum Completion Time	Sum/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.
Detailed result information	Displays detailed result information.

Display the result of an NQA UDP 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
   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: 2014-09-01 10:47:57+08:00
   End time: 2014-09-01 10:48:01+08:00
```

Table 16-60 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.

Item	Description
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 test result is obtained or no test result is obtained after the test. • failed: indicates that the test fails.
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.
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.

Item	Description
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.
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.

Item	Description
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.
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 Number	Number of out-of-order fragmented 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.

Item	Description
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.
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.
Start time	Time when the test began.
End time	Time when the test ended.

16.7.13 display nqa-agent

Function

The **display nqa-agent** command displays the status and configuration of the specified or all NQA test instances 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

After the test instances are configured on an NQA client, run the **display nqa-agent** command to view the status and configuration of the specified or all NQA test instances on an NQA client.

Example

Display the status and configuration of all NQA test instances on an NQA client.

```
<HUAWEI> display nqa-agent
nqa test-instance admin ftp
 test-type ftp
 ftp-operation get
 nqa status : normal
nqa test-instance admin icmp
 nqa status : normal
nqa test-instance admin jitter
 test-type jitter
 destination-address ipv4 10.10.10.10
 destination-port 100
 nqa status : normal
```

Table 16-61 Description of the **display nqa-agent** command output

Item	Description
nqa test-instance admin icmp test-type icmp destination-address ipv4 192.168.1.2 nqa status : normal	The administrator of NQA test instance **icmp** is **admin**. Configurations of this test instance include the following: • test-type • destination-address • nqa status You can run the **nqa** command to configure an NQA test instance. Configurations of different NQA test instances are not the same. For details, see **Configuring an NQA Test Instance**.

16.7.14 display nqa-server

Function

The **display nqa-server** command displays information about NQA servers.

Format

display nqa-server

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display nqa-server** command can display information about NQA servers, including the maximum number of configurable NQA servers and the number and types of configured NQA servers.

Example

Display the information about NQA servers.

```
<HUAWEI> display nqa-server
NQA Server Max:100                    NQA Server Num:3
NQA Concurrent TCP Server:1             NQA Concurrent UDP Server:2
 nqa-server tcpconnect 10.1.1.1 2000   ACTIVE
 nqa-server udpecho 10.1.1.1 2000      ACTIVE
 nqa-server udpecho 10.1.1.1 6000      ACTIVE
```

Table 16-62 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-server	Running servers.
ACTIVE	Status of the NQA server.

16.7.15 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**.

```
<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
```

16.7.16 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 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 type of test instances that are not supported is as follows:

- FTP
- Trace
- LSP Trace
- PWE3 Trace
- DNS
- Path Jitter
- Path MTU

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
```

16.7.17 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 once.

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 once at each configured interval. Configuring the interval of periodic NQA test avoids time-consuming manual operations.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Configuration Impact

If the master/slave switchover is performed on the NQA client before the test instance (group) is complete, the following situations may occur:

- If the interval for automatically performing the test is not set, the test stops after the master/slave switchover.
- If the interval for automatically performing the test instance is set, the test is performed from the next period after the master/slave switchover.

Precautions

- The frequency of a running test instance cannot be changed.
- In a trace, Path MTU, LSP trace, or PWE3 trace test, the configured **frequency** must be greater than or equal to 60s.
- The configured **frequency** cannot be less than the **timeout** value, otherwise, the test instance will start failed. If the configured **frequency** is smaller than or equal to (**probe-count** - 1) x **interval** + **timeout** + 1, the test result may be **no result**. For the test instance supporting the **jitter-packetnum** parameter, the number of sent packets is **probe-count** x **jitter-packetnum** packets.
- In an FTP test instance, the configured **frequency** must be 2s greater than the **timeout** value; otherwise, the FTP test instance may fail.

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
```

16.7.18 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

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
```

16.7.19 ftp-filesize

Function

The **ftp-filesize** command sets the size of the file used in an NQA FTP test instance.

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
```

16.7.20 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

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
```


16.7.21 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. ● If the password is plaintext, the length ranges from 1 to 32. ● If the password is ciphertext, the length 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.

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 68 case-sensitive characters without spaces. ● If the password is plaintext, the length ranges from 1 to 32. ● If the password is ciphertext, the length 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 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 **Tester-123**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type ftp
[HUAWEI-nqa-user-test] ftp-password Tester-123
```

16.7.22 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

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
```

16.7.23 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

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
```

16.7.24 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

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.	The total length of *verstring* should be equal to or shorter than 7 characters. 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.

When running the **http-url** command, you need to specify a domain name or a server's IP address; otherwise, the test instance fails.

Example

Set the URL of HTTP test instance **user test** to **http://www.***.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.***.com
```

16.7.25 icmp-jitter-mode

Function

The **icmp-jitter-mode** command specifies the mode of an ICMP jitter test.

The **undo icmp-jitter-mode** command restores the default mode of an ICMP jitter test.

By default, the ICMP jitter test is in **icmp-timestamp** mode.

Format

icmp-jitter-mode { **icmp-echo** | **icmp-timestamp** }

undo icmp-jitter-mode

Parameters

Parameter	Description	Value
icmp-echo	Configures the ICMP jitter test to use ICMP Echo messages.	-
icmp-timestamp	Configures the ICMP jitter test to use ICMP Timestamp messages.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **icmp-jitter-mode** command can only be used to configure the mode for ICMP jitter or path jitter tests.

Example

Configure the ICMP jitter test to use ICMP Echo messages.

```
<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
```

16.7.26 interval (NQA view)

Function

The **interval** command sets the interval at which NQA test packets are sent.

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

By default, the intervals for sending test packets in various tests are as follows:

- For UDP Jitter, Path Jitter, and ICMP Jitter test instance, the interval is 50 milliseconds on the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S and is 100 milliseconds for other devices.
- 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 20 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

The type of a test instance has been specified using the **test-type** command. The **interval** command is valid only for the ICMP, ICMP Jitter, Path Jitter, SNMP, LSP Jitter, LSP Ping, PWE3 Ping, TCP, UDP, or UDP Jitter test instances.

Configuration Impact

- Packets can be sent at interval of milliseconds only in UDP Jitter, Path Jitter, or ICMP 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 UDP Jitter, Path Jitter, or ICMP 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.

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
```

16.7.27 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

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

Only ICMP test instances support this configuration.

If you configure both the **ip-forwarding** and **sendpacket passroute** commands, the **sendpacket passroute** command takes effect. Therefore, the device sends packets without searching the routing table.

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
```

16.7.28 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

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 UDP Jitter, LSP jitter, Path Jitter, and ICMP Jitter test instances.

Configuration Impact

- In UDP Jitter, LSP jitter, Path Jitter, and ICMP 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
```

16.7.29 local-pw-id

Function

Using the **local-pw-id** command, you can set the ID of the local end of a PW or a VC.

Using the **undo local-pw-id** command, you can delete the configured ID of the local end of a PW or a VC.

By default, **local-pw-id** is not configured.

Format

local-pw-id *local-pw-id*

undo local-pw-id

Parameters

Parameter	Description	Value
local-pw-id	Specifies the ID of the local end of a PW or a VC.	The value is a decimal integer. • When the test instance is of PWE3Ping, the value of *local-pw-id* is an integer that ranges from 1 to 4294967295, and only the VC type of LDP is supported. • When the test instance is of PWE3Trace: when the VC type is LDP, the value of *local-pw-id* is an integer that ranges from 1 to 4294967295; when the VC type is BGP, the value of *local-pw-id* is an integer that ranges from 0 to 65534.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PWE3 ping and PWE3 trace test instances can be used in the following scenarios:

Connectivity and faulty node detections for a single-hop PW. After the **local-pw-id** command is run in the NQA view to configure the local PW ID or VC ID, you can specify a PW for the detection.

Connectivity and faulty node detections for a multi-hop PW. After the **local-pw-id** command is run in the NQA view to configure the local PW ID or VC ID, you need to specify the destination address.

- If the **label-type** parameter is set to **control-word**, run the **remote-pw-id** *remote-pw-id* command to configure the remote PW ID.
- If the **label-type** parameter is set to **label-alert** or **normal**, run the **destination-address ipv4** *ipv4-address* [**lsp-masklen** *masklen* | **lsp-masklen** *masklen* **lsp-loopback** *loopback-address* | **lsp-loopback** *loopback-address* **lsp-masklen** *masklen*] command to configure the destination address for PWE3 ping and PWE3 trace test instances.

Prerequisites

Before running the **local-pw-id** command, you must set the NQA test type to PWE3 Trace or PWE3 Ping in the NQA view.

Precautions

The *local-pw-id* value must be the same as the **VC ID** value in the **display mpls l2vc** command output; otherwise, the test may fail.

Example

Set the ID of the local end of a PW to 100 in the NQA view.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance admin pwe3
[HUAWEI-nqa-admin-pwe3] test-type pwe3trace
[HUAWEI-nqa-admin-pwe3] local-pw-id 100
```

16.7.30 local-pw-type

Function

Using the **local-pw-type** command, you can configure the PW type of the local end.

Using the **undo local-pw-type** command, you can cancel setting the PW type of the local end.

By default, the PW type of the local end is Ethernet.

Format

local-pw-type *local-pw-type*

undo local-pw-type

Parameters

Parameter	Description	Value
local-pw-type	Specifies the PW type of the local end.	Currently, encapsulation types **ethernet**, **ip-interworking** and **vlan**are supported. By the default, the value is **ethernet**.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **local-pw-type** command is used to configure a PW encapsulation type for the local PE. The PW encapsulation type configured for the local PE must be the same as the PW encapsulation type for the remote PE.

Prerequisites

Before configuring the **local-pw-type** command, configure the test type of NQA test instances as PWE3 trace or PWE3 ping in the NQA view.

Precautions

The *local-pw-type* value must be the same as the **VC type** value in the **display mpls l2vc** command output; otherwise, the test may fail.

Example

In the NQA view, configure the local pw-type as VLAN.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance admin pwe3
[HUAWEI-nqa-admin-pwe3] test-type pwe3trace
[HUAWEI-nqa-admin-pwe3] local-pw-type vlan
```

16.7.31 label-type

Function

Using the **label-type** command, you can configure the label type.

Using the **undo label-type** command, you can cancel the operation of configuring the label type.

By default, the label type is **control-word**.

Format

label-type { **control-word** | { **label-alert** | **normal** } [**no-control-word**] }

undo label-type

Parameters

Parameter	Description	Value
control-word	Indicates that the control word option is encapsulated in MPLS Echo Request packets.	-
label-alert	Indicates that the router alert option is encapsulated in MPLS Echo Request packets.	-
normal	Indicates that neither control words nor router alert options are encapsulated in MPLS Echo Request packets.	-
no-control-word	Indicates that the control word option is not encapsulated in MPLS Echo Request packets. This parameter can be used in NQA PWE3 ping and NQA PWE3 trace tests.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The usage scenarios of the label types are as follows:

- **control-word**:
  - If the encapsulation type is set to **control-word**, at a switch node on a multi-hop PW, the MPLS Echo Request packets are not delivered to the CPU for processing until the TTL of the label times out. In this case, the source obtains little PW information. This type, however, ensures system performance and the source cannot learn information on the downstream interfaces of the switch node. You should use this type when there are a great number of packets.
  - Only **control-word** is supported when the vc-type is BGP and lsp-version is draft6.
- **label-alert**:

  - If the encapsulation type is set to **label-alert**, at a switch node on a multi-hop PW, the MPLS Echo Request packets are delivered to the CPU for processing. In this case, the source can obtain more PW information. The system performance is greatly affected when there are a great number of packets. You can use this type to obtain details about the switch node when test instances are few.
  - Only **control-word** or **label-alert** is supported when the vc-type is BGP and lsp-version is rfc4379.
- In the case that a device communicates with Huawei devices running earlier versions and the label alert or normal mode is adopted, the **no-control-word** option must be carried in the test packets.
- **normal** is unsupported when the lsp-version is draft6.

Prerequisites

Before running the **label-type** command, you must set the test type to PWE3 Trace or PWE3 Ping in the NQA view; otherwise, **label-type** cannot be specified.

Precautions

The **label-type** value must be the same as the **local VCCV** value in the **display mpls l2vc** command output; otherwise, the test may fail.

Example

Configure the encapsulation type of test packets as **label-alert** in the NQA view.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance admin pwe3
[HUAWEI-nqa-admin-pwe3] test-type pwe3trace
[HUAWEI-nqa-admin-pwe3] label-type label-alert
```

16.7.32 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

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

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
```

16.7.33 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

Two conditions must be met before you use the command:

- **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
- LSP Jitter

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
```


16.7.34 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** }

undo lsp-replymode

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. Meanwhile, 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.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Using the **lsp-replymode** command, you can set the reply mode for the LSP test. The supported test instances are:

- LSP Ping
- LSP Trace
- LSP Jitter

- PWE3 Ping
- PWE3 Trace

Precautions

lsp-replymode no-reply indicates the unidirectional test. If the client displays timeout, it indicates that the test succeeds; or the client displays that the LSP is non-existent.

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
```

16.7.35 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

Usage Guidelines

Usage Scenario

Hot standby: An ordinary backup CR-LSP is set up immediately after a primary CR-LSP is set up. The ordinary backup CR-LSP takes over traffic if the primary CR-LSP fails. After the primary CR-LSP recovers, traffic switches back.

CR-LSP backup can be configured to allow traffic to switch from a primary CR-LSP to a backup CR-LSP, providing end-to-end protection.

An NQA LSP test instance can check the reachability of the following LSPs and collect SLA statistics:

- MPLS TE tunnel: Run the **lsp-tetunnel** *interface-type interface-number* command to configure an interface number for an MPLS TE tunnel.
- Hot-standby MPLS CR-LSP: Run the **lsp-tetunnel** *interface-type interface-number* **hot-standby** command to configure an interface number for a hot-standby MPLS CR-LSP.
- Primary MPLS TE tunnel: Run the **lsp-tetunnel** *interface-type interface-number* **primary** command to configure an interface number for a primary MPLS TE tunnel.

Prerequisites

Before using the **lsp-tetunnel** command to configure the TE tunnel in an NQA LSP test instance, perform the following operations:

- Run the **interface tunnel** *interface-number* command to create a tunnel interface.
- Run the **lsp-type te** command to set the NQA LSP test type to TE.

Precautions

LSP Jitter test instances cannot test the hot-standby tunnel of a TE tunnel.

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 1
[HUAWEI-Tunnel1] 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 1
```

Configure the CR-LSP hot-standby tunnel of the test named **user test**.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] 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 1 hot-standby
```


16.7.36 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

Parameters

Parameter	Description	Value
ipv4	Sets the test type to IPv4 LSP ping/trace/jitter.	-
te	Sets the type to LSP ping/trace/jitter 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

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, LSP trace, or LSP jitter.
- If the LSP test type is set to TE, the NQA test instance type must be set to LSP ping, LSP trace, or LSP jitter.
- If the LSP test type is set to IPv4 L3VPN, the NQA test instance type must be set to LSP ping.

Precautions

The type of an LSP test that is running cannot be changed.

After the **lsp-type** command is configured, the **destination-address**, **lsp-tetunnel**, and **lsp-version** commands cannot be configured.

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
```

16.7.37 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** }

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.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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**, **lsptrace**, **lspjitter**, **pwe3ping**, or **pwe3trace** 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
```

16.7.38 md

Function

Using the **md** command, you can specify the Maintenance Domain (MD) and Maintenance Association (MA) of the NQA test packet to be sent. This command takes effect only in the MAC Ping test instance.

Using the **undo md** command, you can remove the specified MD from the NQA test packet to be sent.

By default, no MD is specified.

Format

md *md-name* **ma** *ma-name*

undo md

Parameters

Parameter	Description	Value
md-name	Specifies an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces.

Parameter	Description	Value
ma-name	Specifies an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to specify the MD and MA of an MAC Ping test instance. This command has the same effect as the operation of checking the connectivity fault in the MA view. Before running this command, you need to create an MD and MA, and set the test type to macping.

You cannot modify the MD and MA when the test instance is running. The total length of *ma-name* and *md-name* combination cannot be greater than 44 characters.

Example

Set the test type of an NQA test instance to MAC Ping and specify the MD name to "mdcustomer" and the MA name to "macustomer".

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type macping
[HUAWEI-nqa-user-test] md mdcustomer ma macustomer
```

16.7.39 mep

Function

Using the **mep** command, you can configure the MEP ID for an NQA test instance.

Using the **undo mep** command, you can delete the MEP ID configured for an NQA test instance.

By default, the MEP ID for an NQA test instance is 0.

Format

mep mep-id *mep-id*

undo mep

Parameters

Parameter	Description	Value
mep-id	Specifies the MEP ID of an NQA test instance.	The value is an integer ranging from 1 to 8191.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Before starting an NQA test instance, you need to run the **mep-id** *mep-id* command to configure the EOAM module. Otherwise, the normal operation of the NQA test instance will be affected.

This command is available for NQA MAC ping test instances.

Example

Set the MEP ID of an NQA MAC ping test instance to 1.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance test macping
[HUAWEI-nqa-test-macping] test-type macping
[HUAWEI-nqa-test-macping] mep mep-id 1
```

16.7.40 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

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 configure a next hop address for an NQA ICMP test instance, the test instance packets will be sent based on the address.

You can also run the **source-interface** command to specify an outbound interface through which the NQA ICMP test instance packets are sent to the specified next hop address. To guarantee that the test packets are sent, the following two conditions must be met:

- The specified next hop address matches the outbound interface.
- The specified outbound interface cannot be the member interface of a logical interface.

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
```

16.7.41 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 characters without question marks (?), spaces, or hyphens (-). **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 characters without question marks (?), spaces, or hyphens (-). **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.
all-test-instance	Specifies all NQA test instances.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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 except the running test instance will be deleted.

Precautions

A running test instance cannot be deleted.

Example

Create a test named **user test**.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test]
```

16.7.42 nqa-jitter tag-version

Function

The **nqa-jitter tag-version** command sets the packet version for a UDP Jitter test instance.

The **undo nqa-jitter tag-version** command restores the default packet version for a UDP Jitter test instance.

By default, the packet version of a UDP 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 UDP 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 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 UDP Jitter test instance has been configured, running the **nqa-jitter tag-version** command will override the previous configuration.

Precautions

No matter the version number of the UDP Jitter test packet is 1 or 2, you need to run the **nqa-server udpecho** command to configure the NQA server. Otherwise, the UDP Jitter test instance will fail due to timeout.

Example

Set the packet version of a UDP Jitter test instance to 2.

```
<HUAWEI> system-view
[HUAWEI] nqa-jitter tag-version 2
```

16.7.43 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* }

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 must be an existing VPN instance name.
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.
- 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
```

16.7.44 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*] { *ip-address* | **ipv6** *ipv6-address* } *port-number*

undo nqa-server udpecho { [**vpn-instance** *vpn-instance-name*] { *ip-address* | **ipv6** *ipv6-address* } *port-number* | **all** }

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.	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

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 UDP 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 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.

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 client and the server are connected through a VPN, you need to specify the VPN instance name.

No matter the version number of the UDP Jitter test packet is 1 or 2, you need to configure the NQA server. Otherwise, the UDP Jitter test instance 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
```

16.7.45 peer-address (NQA view)

Function

The **peer-address** command specifies a peer IP address for an NQA PWE3 ping or trace test instance.

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

By default, no peer IP address is specified for an NQA PWE3 ping or trace test instance.

Format

peer-address *peer-address*

undo peer-address *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies a peer IP address for an NQA PWE3 ping or trace test instance.	The value is in dotted decimal notation.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

For an NQA PWE3 ping or trace test instance, if the primary and secondary VCs are configured with the same VC ID, the **peer-address** command must be configured to specify a peer IP address. This configuration determines a unique PW for the NQA test.

Example

Specify 10.1.1.1 as the peer IP address of an NQA PWE3 ping test instance.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type pwe3ping
[HUAWEI-nqa-user-test] peer-address 10.1.1.1
```

16.7.46 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.

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. The type of test instances that are not supported is as follows:

- FTP
- DNS

Configuration Impact

- In UDP Jitter test instances, ICMP Jitter test instances, Path Jitter test instances, LSP 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 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
```

16.7.47 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. Path jitter and Path MTU test are not supported.

Follow-up Procedure

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**, you are advised to set **probe-failtimes** to 1; otherwise, traps cannot be sent.

If the test instance supports **probe-count**, 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
```

16.7.48 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.

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 1000. 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. Path MTU test is not supported.

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
```

16.7.49 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

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before running the **remote-pw-id** command, you must set the test type to PWE3 Trace or PWE3 Ping in the NQA view.

Precautions

You cannot configure the **remote-pw-id** command after setting **lsp-version** to **rfc4379**.

The *remote-pw-id* value must be the same as the **VC ID** value in the **display mpls l2vc remote-info verbose** command output; otherwise, the test may fail.

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
```


16.7.50 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
```

16.7.51 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.

Format

sendpacket passroute

undo sendpacket passroute

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

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
- UDP Jitter
- FTP
- SNMP
- Trace

Precautions

You cannot change this configuration of a running test instance.

If you configure both the **sendpacket passroute** and **source-interface** commands, the **source-interface** command takes effect. In this scenario, packets are sent from the interface specified using the **source-interface** command.

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
```

16.7.52 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** | { **probefailure** | **rtd** | **testcomplete** | **testfailure** | **testresult-change** } * }

undo send-trap { **all** | { **probefailure** | **rtd** | **testcomplete** | **testfailure** | **testresult-change** } * }

Parameters

Parameter	Description	Value
all	Indicates that a trap is sent in any of the following situations: ● The RTD exceeds the threshold. ● NQA probes fail. ● An NQA test succeeds. ● NQA tests fail.	-
probefailure	Indicates that a trap is sent when the number of probe failures reaches the threshold. **NOTE** This parameter does not apply to the UDP Jitter and ICMP 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.	-
testfailure	Indicates that a trap is sent when the number of test failures reaches 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 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.

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.

probefailure indicates that a trap is sent when the number of probe sending failures reaches the threshold set using the **probe-failtimes** command within a detection period. **testfailure** indicates that all probes fail to be sent within a detection period. When the number of detection failures reaches the threshold set using the **test-failtimes** command, a trap is sent. For example, if three probes are sent in a detection period and probe-failtimes and test-failtimes are set to 1, the alarm specified by probefailure is triggered when one probe fails to be sent and two probes are successfully sent. If all the three probes fail to send packets, the alarm specified by testfailure is triggered.

Prerequisites

The type of a test instance has been specified using the **test-type** command. Path jitter and Path MTU test are not supported.

The route between the device and NMS is reachable, and related configurations are complete. The host where traps are sent is configured using the **snmp-agent target-host trap** 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
```

16.7.53 sender-address

Function

The **sender-address** command configures the source IP address in the multi-hop PW scenario.

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

By default, no source IP address is configured.

Format

sender-address ipv4 *ip-address*

undo sender-address

Parameters

Parameter	Description	Value
ipv4 *ip-address*	Specifies a source IPv4 address.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When PWE3 ping is performed in the multi-hop PW scenario, and the *lsp-version* is **rfc4379**, the **sender-address** command specifies a source IP address. The value is a routable address on the same public network with the address of the destination PE. Usually, the source IP address is the address of the adjacent SPE or UPE.

Precautions

After the **sender-address** command is run, the LSP version cannot be set to **draft6**.

Example

Set the source IP address of the PWE3 ping test instance in the multi-hop PW scenario to 10.1.1.1.

```
<HUAWEI> system-view
```



```
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type pwe3ping
[HUAWEI-nqa-user-test] lsp-version rfc4379
[HUAWEI-nqa-user-test] sender-address ipv4 10.1.1.1
```

16.7.54 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

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
```

16.7.55 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*

source-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 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

Usage Guidelines

Usage Scenario

After the test packets are transmitted to the destination address, the source address of the NQA test instance is used as the destination address. The **source-address** command is used to configure the source IP address for the NQA test. 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 PWE3 trace, PWE3 ping, or MAC ping.

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
```

16.7.56 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

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 ICMP, ICMP Jitter, UDP Jitter, Path MTU, and MAC Ping test instances.

Precautions

The configuration of the source interface of a running test instance cannot be changed.

The source interface of an NQA test instance must be an interface with an IP address configured; otherwise, the command cannot take effect.

The source interface cannot be a link aggregation interface or a member interface in load balancing scenario; otherwise, the command cannot take effect.

Example

Set the source interface of test instance **user test** to vlanif 100.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type icmp
[HUAWEI-nqa-user-test] source-interface vlanif 100
```

16.7.57 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

The test instance type has been specified using the **test-type** command. The source port can be configured for FTP, HTTP, SNMP, UDP Jitter, TCP, and UDP test instances.

Precautions

The port specified in the **source-port** command must be available; otherwise, the probe fails.

Ports in the range from 61441 (excluded) to 65535 are reserved and cannot be used. 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
```

16.7.58 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

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).

Parameter	Description	Value
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. **NOTE** The delay in stopping a test instance must be set to at least 6s later than the delay in performing the test instance.
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. Although this command has been run and configurations have been saved, this **start now** command will not be restored and needs to be run again after the device is restarted.

When starting a test instance at a specified time, the time must be later than the current time on the device.

If no end time is configured, the test cannot stop automatically. You need to stop it manually using the **stop** command.

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
```

16.7.59 step (NQA view)

Function

Using the **step** command, you can set the value of the incremental step for the packet length in the path MTU test.

Using the **undo step** command, you can delete the current setting.

By default, the value of the incremental step is 10.

Format

step *step*

undo step

Parameters

Parameter	Description	Value
step	Specifies the value of the incremental step.	It is an integer ranging from 1 to 512, in bytes. The default value is 10 bytes.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **step** command is run to set the value of the incremental step for the packet length, only when the test type is configured as the path MTU test.

Example

Set the value of the incremental step for the packet length in the path MTU test to 50 bytes.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type pathmtu
[HUAWEI-nqa-user-test] step 50
```

16.7.60 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
```

16.7.61 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. Path jitter and Path MTU test are not supported.

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.

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
```

16.7.62 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 { **dns** | **ftp** | **http** | **icmp** | **icmpjitter** | **jitter** | **lspjitter** | **lspping** | **lsptrace** | **macping** | **pathjitter** | **pwe3ping** | **pwe3trace** | **snmp** | **tcp** | **trace** | **udp** | **pathmtu** }

undo test-type

NOTE

Only the S5731-H, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support **lspjitter**, **lspping**, **lsptrace**, **pwe3ping**, and **pwe3trace**.

Parameters

Parameter	Description	Value
dns	Specifies a DNS test.	-
ftp	Specifies an FTP service test.	-
http	Specifies an HTTP service test.	-

Parameter	Description	Value
icmp	Specifies an ICMP test.	-
icmpjitter	Specifies an ICMP jitter test, which can detect the jitter on the network.	-
jitter	Specifies a UDP jitter test, which can detect the jitter during UDP packet transmission.	-
lspjitter	Specifies an LSP jitter test.	-
lspping	Specifies an LSP ping test.	-
lsptrace	Specifies an LSP trace route test.	-
macping	Specifies a MAC ping test.	-
pathjitter	Specifies a path jitter test, which can detect the hop-by-hop jitter during the ICMP packet transmission.	-
pwe3ping	Specifies a PWE3 ping test.	-
pwe3trace	Specifies a PWE3 trace test.	-
snmp	Specifies an SNMP test.	-
tcp	Specifies a TCP test.	-
trace	Specifies a trace test.	-
udp	Specifies a UDP test.	-
pathmtu	Specifies a path MTU test to find the minimum MTU value on the network.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

- After an NQA test instance is created, a test type needs to be specified for it as other parameters are configured based on the test instance type. To configure the test type for an NQA test instance, run the **test-type** command.
- You cannot change the type of a running test instance.
- An ICMP test is usually conducted to check the connectivity. However, it cannot accurately test the link delay. Therefore, to test link delay or other link performance, you are advised to conduct an ICMP jitter or UDP jitter test.

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
```

16.7.63 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

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

This command applies to the ICMP Jitter and UDP Jitter tests.

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] timestamp-unit microsecond
```

16.7.64 threshold

Function

The **threshold** command sets the RTD threshold.

The **undo threshold** command deletes the RTD threshold.

By default, no threshold is set.

Format

threshold rtd *rtd-value*

undo threshold rtd

Parameters

Parameter	Description	Value
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 type of a test instance has been specified using the **test-type** command. Path jitter and Path MTU test are test is not supported.

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
```

16.7.65 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 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 test fails. The timeout period is set based on the actual networking.

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.
- 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.

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
```

16.7.66 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.

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 supported:

- FTP
- HTTP
- ICMP
- ICMP Jitter
- UDP Jitter
- SNMP
- TCP
- UDP

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
```

16.7.67 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 indicate 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 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
```

16.7.68 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 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
```

16.7.69 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
- Trace
- MAC Ping
- Path Jitter
- Path MTU

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
```

16.7.70 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

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 PWE3 networks and 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 a 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
```

16.7.71 undo no-control-word

Function

Using the **undo no-control-word** command, you can enable the control-word option.

By default, the control-word is used in packet encapsulation.

Format

undo no-control-word

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The control-word option carries control-word information in each encapsulated packet. The information is used for packet sequence verification, packet fragmentation, and packet reassembling on the forwarding plane.

By default, the control-word is used in packet encapsulation. If a non-huawei device does not support control-word information in the packet structure, the **label-type** { { **label-alert** | **normal** } **no-control-word** } command can be used on the Huawei device to remove the control-word option from each packet sent to the non-huawei device to facilitate their interworking.

If a non-huawei device supports control-word information in the packet structure, the **undo no-control-word** command can be used on the Huawei device to restore the Huawei packet structure.

NOTE

Only PWE3 Ping and PWE3 Trace test instances support the **undo no-control-word** command.

Example

Enable the control-word option.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance user test
[HUAWEI-nqa-user-test] test-type pwe3ping
[HUAWEI-nqa-user-test] label-type label-alert no-control-word
[HUAWEI-nqa-user-test] undo no-control-word
```

16.7.72 vc-type

Function

Using the **vc-type** command, you can configure the type of the protocol used for setting up an L2VPN VC in the NQA view.

Using the **undo vc-type** command, you can delete the protocol type configured in the NQA view.

By default, the type of the protocol used for setting up an L2VPN VC is LDP.

Format

vc-type { **ldp** | **bgp** }

undo vc-type

Parameters

Parameter	Description	Value
ldp	Propagates inner labels by using LDP as the signaling protocol.	-
bgp	Propagates inner labels by using BGP as the signaling protocol.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **vc-type** command is used to configure the signaling protocol for an NQA test instance to be identical with that for the PW on the network to be tested.

Prerequisites

For the **vc-type ldp** command, ensure that the test instance is of the following type:

- PWE3 Ping
- PWE3 Trace

For the **vc-type bgp** command, ensure that the test instance is of the following type:

- PWE3 Trace

Precautions

The signaling type of a running test instance cannot be changed.

Example

In the NQA view, configure BGP to be the type of the protocol used for setting up an L2VPN VC.

```
<HUAWEI> system-view
[HUAWEI] nqa test-instance admin pwe3
[HUAWEI-nqa-admin-pwe3] test-type pwe3trace
[HUAWEI-nqa-admin-pwe3] vc-type bgp
```

16.7.73 vpn-instance (NQA view)

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.

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 must be an existing VPN instance name.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **vpn-instance** command applies to FTP, HTTP, ICMP, ICMP Jitter, Path Jitter, SNMP, TCP, trace, UDP, Path MTU, and UDP Jitter test instances.

In a PWE3 Trace test instance, if the protocol type of the L2VPN VC is set to BGP by the **vc-type** command, you can run the **vpn-instance** command to specify a VPN instance name for the PWE3 Trace test instance.

You cannot change this configuration of a running test instance.

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
```

16.8 Service Diagnosis Configuration Commands

16.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.8.2 display trace information

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, such as the number of diagnosis instances and the number of diagnosis 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            : -
Terminal process enable             : On
Authentication duration threshold   : 10s
AAA duration threshold              : 5s
CM duration threshold               : 5s

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 16-63 Description of the **display trace information** command output

Item	Description
Trace Information	Information about service diagnosis.

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	Source IP address of the interface for exporting diagnosis information to the log server. To set this parameter, run the **trace syslog source** command.
Terminal process enable	Whether the function of logging the network access process and interaction packets of terminals is enabled. ● Disable: This function is disabled. ● Enable: This function is enabled. To configure this function, run the **trace object process enable** command.
Authentication duration threshold	Threshold of the processing time for the access module during terminal authentication.
AAA duration threshold	Threshold of the processing time for the AAA module during terminal authentication.
CM duration threshold	Threshold of the processing time for the CM module during terminal authentication.
The sum of all the instances	Total number of diagnosis instances.

Item	Description
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 released diagnosis instances.
The sum of all the objects	Total number of diagnosis objects.

16.8.3 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*] [**process-wlan**]

NOTE

The **process-wlan** keyword is only supported by S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H.

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 1 to 4 digits.

Parameter	Description	Value
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 must be an existing VPN instance name.
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.
process-wlan	Specifies the WLAN sub-core.	-

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-fc12-3456
  IP Flag        : -
  Session ID     : -
```



```
IP Address     : 10.10.10.1
VRF Index      : -
CID            : 100
User Name      : -
Interface      : -
QinQ VLAN ID   : -
User VLAN ID   : -
Access Mode    : dot1x
Modules online : EAPoL  :0    WEBS   :0       WEB    :0       AAA    :0
                 CM     :0    TM     :0       SAM    :0       RADIUS :1
                 DHCPS  :0    DHCPC  :0       DHCPR  :0       DHCPP  :0
                 TACACS :0    AM     :0       SAVI   :0       WLAN_AC:0
------------------------------------------------------------------
Total 1, 1 printed
```

Table 16-64 Description of the display trace instance command output

Item	Description
ID	ID of the diagnosis instance.
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 VPN instance index.
CID	User connect ID.
User Name	User name.
Interface	Interface index.
QinQ VLAN ID	QinQ VLAN ID.
User VLAN ID	User VLAN ID.
Access Mode	User access mode, including dot1x, mac-authen, portal, and wlan. To set the user access mode, run the **trace object** command.
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.

16.8.4 display trace object

Function

The **display trace object** command displays the configuration about a service diagnosis object.

Format

display trace object [*service-object-id*]

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.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you do not specify *service-object-id*, configurations about all diagnosis objects are displayed.

Example

Display configurations about all diagnosis objects.

```
<HUAWEI> display trace object
Trace Object Syslog Server:
  SSL_Policy     : test
  Port           : 6514
Trace Object:
------------------------------------------------------------------
  Object ID      : 0
  Slot           : -
  MAC Address    : -
  IP Flag        : -
  Session ID     : -
  IP Address     : 10.1.1.1
  VRF Index      : -
  CID            : -
  User Name      : -
  Interface      : -
  QinQ VLAN ID   : -
  User VLAN ID   : -
  Access Mode    : -
  User Tunnel ID : -
  Output         : command line ( User-Intf 4 )

  Object ID      : 1
  Slot           : -
  MAC Address    : 00e0-fc01-0101
  IP Flag        : -
  Session ID     : -
  IP Address     : -
  VRF Index      : -
  CID            : -
  User Name      : -
  Interface      : -
```



```
QinQ VLAN ID   : -
User VLAN ID   : -
Access Mode    : -
User Tunnel ID : -
Output         : file ( flash:/a.txt )

Object ID      : 2
Slot           : -
MAC Address    : 00e0-fc01-0101
IP Flag        : -
Session ID     : -
IP Address     : 10.2.2.2
VRF Index      : -
CID            : -
User Name      : -
Interface      : -
QinQ VLAN ID   : -
User VLAN ID   : -
Access Mode    : -
User Tunnel ID : -
Output         : server ( 10.10.10.10 )

--------------------------------------------------------------
Total 3, 3 printed
```

Table 16-65 Description of the **display trace object** command output

Item	Description
Object ID	ID of a diagnosis object. This parameter is automatically generated from 0 in sequence of creation time.
Slot	Slot ID of the device.
MAC Address	MAC address. To set this parameter, 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 this parameter, run the **trace object** command.
VRF Index	User VRF index.
CID	User CID.
User Name	User name. To set this parameter, run the **trace object** command.
Interface	Interface index. To set this parameter, run the **trace object** command.
QinQ VLAN ID	QinQ VLAN ID. To set this parameter, run the **trace object** command.
User VLAN ID	User VLAN ID. To set this parameter, run the **trace object** command.

Item	Description
Access Mode	User access mode, including dot1x, mac-authen, portal, and wlan. To set this parameter, run the **trace object** command.
Output	Direction in which the device exports diagnosis information. To set this parameter, 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.
Trace Object Syslog Server	Diagnosis information is exported to a log server.
SSL_Policy	Name of an SSL policy. To set this parameter, run the **ssl policy** command. This field is displayed only when the device is enabled to export diagnosis information to a log server and the **trace object output syslog-server** command is run to enable the device to export diagnosis information to the log server using the TLS protocol.
Port	Port number of the log server. This field is displayed only when the device is enabled to export diagnosis information to a log server and the **trace object output syslog-server** command is run to enable the device to export diagnosis information to the log server using the TLS protocol.
Total 3, 3 printed	Total number of created diagnosis objects and number of displayed objects.

16.8.5 reset trace instance

Function

The **reset trace instance** command clears all the diagnosis instances on a device.

Format

reset trace instance

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
```

16.8.6 save trace information

Function

The **save trace information** command saves diagnosis information in the buffer area as a file.

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
```

16.8.7 trace enable

Function

The **trace enable** command enables service diagnosis.

The **undo trace enable** command disables service diagnosis.

By default, service diagnosis is disabled.

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 switch 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.

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
```

16.8.8 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** } } * [**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** } } * [**output** { **command-line** | **file** [*file-name*] | **syslog-server** [*syslog-server-ip*] }]

undo trace object { *service-object-id* | **all** }

NOTE

Only the S5731-H, S5731S-H, S6730S-H, S5732-H, and S6730-H support **access-mode wlan**.

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 1 to 4 digits. If an H contains fewer than 4 digits, the left-most digits are padded with zeros. For example, e0 is displayed as 00e0. The MAC address cannot be set to FFFF-FFFF-FFFF or 0000-0000-0000.
ip-address *ip-address*	Creates a diagnosis object based on the IP address.	The value is in dotted decimal notation.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
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.	-
output	Specifies the direction in which the device exports diagnosis information.	-
command-line	Exports diagnosis information to the CLI.	-

Parameter	Description	Value
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, which is 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.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

When locating faults of DHCP, 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.
- AAA and NAC services: based on the MAC address, IP address, user name, user VLAN ID, or access mode.

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

If a diagnosis object is created based on the MAC address or IP address, various service processes can be diagnosed generally. If a diagnosis object is created based on other parameters, service diagnosis may fail to be performed because the parameters may not be obtained in service processes. Therefore, you are advised to create a diagnosis object based on the MAC address or IP address.

When the **slot** parameter is used for service diagnosis, if a user switches between the pre-authentication connection and authentication success states and authorization information (including ACL, VLAN, or authentication event authorization) is not changed in the switching process, no service diagnosis information will be output. In this situation, you can use the user name or interface for service diagnosis.

The diagnosis output file cannot exceed 5 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** } } * [**output** { **command-line** | **file** [*file-name*] | **syslog-server** [*syslog-server-ip*] }] command. For example, assume that diagnosis objects 1 (10.10.10.1) and 2 (10.10.10.1+00e0-fc12-3456) 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
- Delete all diagnosis objects using the **undo trace object all** command.

Example

Create a diagnosis object on the interface with IP address 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] trace object ip-address 10.10.10.1
```


16.8.9 trace object duration threshold

Function

The **trace object duration threshold** command sets time thresholds for logging the network access process and interaction packets of terminals.

The **undo trace object duration threshold** command cancels the settings of time thresholds for logging the network access process and interaction packets of terminals.

By default, the time threshold for logging temporary entries of the access module during terminal authentication (specified by **authentication**) is 10s; the time threshold for logging user entries of the AAA module during terminal authentication (specified by **aaa**) is 5s; the time threshold for logging the authorization entries delivered by the CM module during terminal authentication (specified by **cm**) is 5s.

Format

trace object { **authentication** | **cm** | **aaa** } **duration threshold** *value*

undo trace object { **authentication** | **cm** | **aaa** } **duration threshold**

Parameters

Parameter	Description	Value
authentication	Specifies the time threshold for logging temporary entries of the access module during terminal authentication.	-
aaa	Specifies the time threshold for logging user entries of the AAA module during terminal authentication.	-
cm	Specifies the time threshold for logging the authorization entries delivered by the CM module during terminal authentication.	-
value	Specifies the time threshold.	The value is an integer in the range from 3 to 180, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To facilitate maintenance and fault locating, you can enable the function of recording the abnormal network access process and interaction packets of terminals in diagnostic log files. However, logs are generated only for the terminals with the network access time exceeding the time thresholds, regardless of whether the terminals are successfully authenticated or fail the authentication. To modify the time thresholds, run the **trace object duration threshold** command.

Prerequisites

The function of logging the abnormal network access process and interaction packets of terminals has been enabled using the **trace object process enable** command.

Precautions

The configuration of the **trace object duration threshold** command is not recorded in the configuration file. Therefore, the function will be disabled after the device is restarted.

Example

In the system view, set the time threshold for logging temporary entries of the access module during terminal authentication to 12s.

```
<HUAWEI> system-view
[HUAWEI] trace object process enable
[HUAWEI] trace object authentication duration threshold 12
```

16.8.10 trace object output syslog-server

Function

The **trace object output syslog-server** command configures the device to export diagnosis information to a log server through TLS.

The **undo trace object output syslog-server** command disables the device from exporting diagnosis information to a log server through TLS.

By default, diagnosis information is not exported to a log server through TLS.

Format

trace object output syslog-server ssl-policy *policy-name* [**port** *port num*]

undo trace object output syslog-server

Parameters

Parameter	Description	Value
ssl-policy *policy-name*	Specifies the name of an SSL policy used to export diagnosis information to a log server. **NOTE** The SSL policy must already exist on the device. If no SSL policy is available, run the **ssl policy** command to create one.	The value is the name of an SSL policy that has been created.
port *port num*	Specifies the port number of a log server.	The value is an integer in the range from 1024 to 65535. The default port number is 6514.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **trace syslog source** command is run, the device transfers diagnosis information to a log server. However, this transfer mode is insecure. In scenarios with high security requirements, you can run the **trace object output syslog-server** command to enable the device to transfer log files to the log server using the TLS protocol.

Prerequisites

A diagnosis object has been created and the device has been enabled to export diagnosis information to a log server using the **trace object** command.

Precautions

The configuration of the **trace object output syslog-server** command is not recorded in the configuration file. Therefore, the function will be disabled after the device is restarted.

If diagnosis information cannot be exported to a log server after the **trace object output syslog-server** command is run, the device automatically puts the log server to the quiet state. The quiet period is 10 minutes. The device does not send diagnosis information to the log server until the quiet period times out. If you want to cancel the quiet state in advance, run the **undo trace enable** or **undo trace object** command. To enable the device to send diagnosis information to the log server again, run the **trace enable** or **trace object** command accordingly.

Example

In the system view, enable the device to export diagnosis information to a log server through TLS.

```
<HUAWEI> system-view
[HUAWEI] ssl policy btr_syslog
[HUAWEI] trace object mac-address 00e0-fc03-0405 output syslog-server 192.168.1.1
[HUAWEI] trace object output syslog-server ssl-policy btr_syslog port 6514
```

16.8.11 trace object process enable

Function

The **trace object process enable** command enables the function of logging the abnormal network access process and interaction packets of terminals.

The **undo trace object process enable** command disables the function of logging the abnormal network access process and interaction packets of terminals.

By default, the function of logging the abnormal network access process and interaction packets of terminals is disabled.

Format

trace object process enable

undo trace object process enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

It is difficult to locate network access issues of terminals on the live network based on debugging information. To facilitate maintenance and fault locating, you can run the **trace object process enable** command to enable the function of recording the abnormal network access process and interaction packets of terminals in a diagnostic log file.

Precautions

The configuration the **trace object process enable** command is not recorded in the configuration file. Therefore, the function will be disabled after the device is restarted.

Example

In the system view, enable the function of logging the abnormal network access process and interaction packets of terminals.

```
<HUAWEI> system-view
[HUAWEI] trace object process enable
```

16.8.12 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 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 VLANIF100 as the source interface for exporting diagnosis information to the log server.

```
<HUAWEI> system-view
[HUAWEI] trace syslog source vlanif 100
```

16.9 Mirroring Configuration Commands

NOTE

The device supports the mirroring function, which is mainly used for network monitoring and fault management and may use user communication information. Huawei will not collect or save user communication information independently. You must use this function in compliance with applicable laws and regulations. Ensure that your customers' privacy is protected when you are using or saving communication information.

16.9.1 Command Support

Model	Port Mirroring	Traffic Mirroring	VLAN Mirroring	MAC Address Mirroring
S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S	Supported	Only local inbound traffic mirroring is supported.	Supported	Supported
S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I	Supported	Only inbound traffic mirroring is supported.	Supported	Supported

Model	Port Mirroring	Traffic Mirroring	VLAN Mirroring	MAC Address Mirroring
S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-H, S6730S-H, S6730-S, S6730S-S	Supported	Supported	Supported	Supported
S6735-S, S6720-EI, S6720S-EI	Supported	Supported	Supported	Supported

16.9.2 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

1: Monitoring level

Usage Guidelines

After observing ports are configured using the **observe-port(local observing port)** or **observe-port(Layer 2 remote observing port)** command in the system view, you can run the **display observe-port** command to check detailed information about the configured observing ports.

Example

Display the observing port configuration.

```
<HUAWEI> display observe-port
 ------------------------------------------------------------------------------
```



```
Index          : 1
Untag-packet   : No
Forwarding     : Yes
Packet-length  : 1000
Interface      : GigabitEthernet0/0/1
------------------------------------------------------------------------------
Index          : 2
Untag-packet   : No
Forwarding     : Yes
Packet-length  : 1000
Interface-range: GigabitEthernet0/0/2
Vlan           : 20
------------------------------------------------------------------------------
Index          : 3
Untag-packet   : No
Forwarding     : Yes
Packet-length  : 1000
Interface-range: GigabitEthernet0/0/3 to GigabitEthernet0/0/5
------------------------------------------------------------------------------
```

Display the observing port configuration (S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S).

```
<HUAWEI> display observe-port
------------------------------------------------------------------------------
Index          : 2
Untag-packet   : No
Forwarding     : Yes
Dynamic-alloc  : No
Interface      : GigabitEthernet0/0/2
------------------------------------------------------------------------------
Index          : 3
Untag-packet   : No
Forwarding     : Yes
Dynamic-alloc  : No
Interface      : GigabitEthernet1/0/3
------------------------------------------------------------------------------
Index          : 4
Untag-packet   : No
Forwarding     : Yes
Dynamic-alloc  : Yes
Interface      : XGigabitEthernet1/0/3
------------------------------------------------------------------------------
```

Table 16-66 Description of the **display observe-port** command output

Item	Description
Index	Index of an observing port.
Untag-packet	Whether to remove VLAN tags of original traffic.
Forwarding	Forwarding parameter value: ● Yes: An observing port can forward data packets. ● No: An observing port does not forward data packets.
Packet-length	Length of the truncated mirrored packet. If the mirrored packet length is not specified when an observing port is configured, this field is not displayed.
Interface	A single observing port.
Interface-range	The observing ports in an observing port group.

Item	Description
Vlan	Layer 2 remote mirroring VLAN.
Dynamic-alloc	Whether the function of dynamically applying for observing port resources is enabled.

16.9.3 display port-mirroring

Function

The **display port-mirroring** command displays the mirroring configuration.

Format

display port-mirroring

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After observing ports and mirrored ports are configured on the switch, you can run the **display port-mirroring** command to check detailed mirroring configuration on the switch.

Example

Display the mirroring configuration.

```
<HUAWEI> display port-mirroring
 ------------------------------------------------------------------------------
 Observe-port 1 : GigabitEthernet0/0/1
 Observe-port 2 : GigabitEthernet0/0/2
 Observe-port 3 : GigabitEthernet0/0/3
 Observe-port 4 : GigabitEthernet0/0/4
 ------------------------------------------------------------------------------
 Port-mirror:
 ------------------------------------------------------------------------------
     Mirror-port               Direction  Observe-port
 ------------------------------------------------------------------------------
 1    GigabitEthernet0/0/15     Inbound    Observe-port 1
 ------------------------------------------------------------------------------
 Stream-mirror:
 ------------------------------------------------------------------------------
```



```
    Behavior                Direction  Observe-port
------------------------------------------------------------------------------
1   b1                      -          Observe-port 2
------------------------------------------------------------------------------
Vlan-mirror:
------------------------------------------------------------------------------
Mirror-vlan             Direction     Observe-port
------------------------------------------------------------------------------
10                      Inbound       Observe-port 3
------------------------------------------------------------------------------
Mac-mirror:
------------------------------------------------------------------------------
Mirror-mac      Vlan    Direction     Observe-port
------------------------------------------------------------------------------
xxxx-xxxx-xxxx  10      Inbound       Observe-port 4
------------------------------------------------------------------------------
```

Table 16-67 Description of the **display port-mirroring** command output

Item	Description
Port-mirror	Port mirroring configuration.
Mirror-port	Mirrored port. This parameter is configured using the **port-mirroring to observe-port** command.
Direction	Direction of mirrored packets: • Inbound • Outbound This parameter is configured using the **port-mirroring to observe-port** command.
Observe-port	Observing port to which mirrored packets are sent. This parameter is configured using the **observe-port(local observing port)** or **observe-port(Layer 2 remote observing port)** command.
Stream-mirror	Traffic mirroring configuration.
Behavior	Traffic behavior of traffic mirroring. • In MQC-based traffic mirroring, this parameter is configured using the **mirroring to observe-port** command. • In ACL-based traffic mirroring, this parameter is configured using the **traffic-mirror** or **traffic-mirror** command.
Vlan-mirror	VLAN mirroring configuration.
Mirror-vlan	VLAN ID in VLAN mirroring. This parameter is configured using the **mirroring to observe-port** command.
Mac-mirror	MAC address mirroring configuration.
Mirror-mac	MAC address in MAC address mirroring. This parameter is configured using the **mac-mirroring** command.

Item	Description
Vlan	VLAN in which MAC address mirroring is used.

16.9.4 mac-mirroring

Function

The **mac-mirroring** command copies packets with a specified MAC address to a specified observing port.

The **undo mac-mirroring** command restores the default configuration.

By default, packets with a specified MAC address are not copied to a specified observing port.

Format

mac-mirroring *mac-address* **to observe-port** *observe-port-index* **inbound**

undo mac-mirroring *mac-address* [**to observe-port** *observe-port-index*] **inbound**

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits.
observe-port-index	Specifies the index of the observing port.	The specified observing port must exist.

Views

VLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In MAC address mirroring, you can run the **mac-mirroring** command to copy packets received with a specified source or destination MAC address in a specified VLAN to a specified observing port.

Prerequisites

An observing port has been configured using the **observe-port(local observing port)** or **observe-port(Layer 2 remote observing port)** command in the system view.

Example

Copy packets received of which the source or destination MAC address is 00e0-fc00-0001 in VLAN 3 to the observing port with index 1.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/1
[HUAWEI] vlan 3
[HUAWEI-vlan3] mac-mirroring 00e0-fc00-0001 to observe-port 1 inbound
```

16.9.5 mirroring to observe-port (VLAN view)

Function

The **mirroring to observe-port** command copies packets received in a specified VLAN to a specified observing port.

The **undo mirroring** command restores the default configuration.

By default, packets received in a VLAN are not copied to any observing port.

Format

mirroring to observe-port *observe-port-index* **inbound**

undo mirroring [**to observe-port** *observe-port-index*] **inbound**

Parameters

Parameter	Description	Value
observe-port-index	Specifies the index of the observing port.	The specified observing port must exist.

Views

VLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In VLAN mirroring, you can run the **mirroring to observe-port** command to copy packets on all the active ports in a specified VLAN to observing ports.

Prerequisites

Observing ports have been configured using the **observe-port(local observing port)** or **observe-port(Layer 2 remote observing port)** command in the system view.

Precautions

For the S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-SX series cards, copying packets received in a specified VLAN to a specified observing port may affect the device forwarding performance (for example, some packets may be discarded during line-rate forwarding when all interfaces are fully loaded). Therefore, exercise caution when using this function.

Example

Copy packets received in VLAN 10 to the observing port with index 1.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/1
[HUAWEI] vlan 10
[HUAWEI-vlan10] mirroring to observe-port 1 inbound
```

16.9.6 mirroring to observe-port (traffic behavior view)

Function

The **mirroring to observe-port** command copies traffic that matches rules to observing ports.

The **undo mirroring** command cancels copying traffic that matches rules to observing ports.

By default, the switch does not copy traffic that matches rules to observing ports.

Format

mirroring to observe-port *observe-port-index*

undo mirroring

Parameters

Parameter	Description	Value
observe-port-index	Specifies the index of the observing port.	The specified observing port must exist.

Views

Traffic behavior view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In traffic mirroring, you can run the **mirroring to observe-port** command to copy traffic that matches rules to specified observing ports.

Prerequisites

Observing ports have been configured using the **observe-port(local observing port)** or **observe-port(Layer 2 remote observing port)** command in the system view.

Precautions

On the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, if selective QinQ, VLAN mapping, flow ID re-marking, 802.1p priority re-marking, or MAC address learning disabling is configured in a traffic behavior, traffic mirroring is not supported.

On the S6720-EI, S6735-S, and S6720S-EI, if flow ID re-marking, re-marking of the inner VLAN tag in QinQ packets, MAC address learning disabling, or redirection of packets to a VPN instance is configured in a traffic behavior, traffic mirroring is not supported.

Example

Copy traffic that matches rules to observing ports with index 1.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/1
[HUAWEI] traffic behavior tb1
[HUAWEI-behavior-tb1] mirroring to observe-port 1
```

16.9.7 observe-port (local observing port)

Function

The **observe-port** command configures local observing ports.

The **undo observe-port** command deletes local observing ports.

By default, no local observing ports are configured.

Format

Configure a single local observing port

observe-port [*observe-port-index*] **interface** *interface-type interface-number* [**untag-packet**] [**truncate packet** *packet-length*]

Configure a local observing port group

observe-port [*observe-port-index*] **interface-range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-n> [**untag-packet**] [**truncate packet** *packet-length*] (Only supported by S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S; n in &<1-n> is 4 on an S6735-S, S6720-EI, and S6720S-EI and 8

on an S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.)

observe-port *observe-port-index* **interface-range** { **add** | **delete** } *interface-type interface-number* (Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

undo observe-port *observe-port-index*

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support **truncate packet** *packet-length*.

Parameters

Parameter	Description	Value
observe-port-index	Specifies the index of an observing port.	The value is an integer. The value ranges from 1 to 8 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, ranges from 1 to 4 on the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, and ranges from 1 to 6 on other devices.
interface-type interface-number	Specifies the type and number of an interface.	-
add	Adds observing ports to the observing port group.	-
delete	Deletes observing ports from the observing port group.	-
untag-packet	Removes VLAN tags of original traffic. **NOTE** Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this parameter. Each original packet can have at most two VLAN tags removed.	-

Parameter	Description	Value
truncate	Truncates packets to be mirrored.	-
packet *packet-length*	Specifies the length of packets to be mirrored.	The value is an integer in the range from 64 to 1023, in bytes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an observing port is directly connected to a monitoring host, you can run the **observe-port** command to configure a local observing port. There are two modes for configuring observing ports: configure a single observing port and configure an observing port group. Observing port group is often used in 1:N mirroring to simplify the configuration and save observing port indexes. This is because an observing port group occupies only one observing port index regardless of how many ports are configured in the group.

Precautions

- The management interface cannot be configured as an observing port.
- If you configure observing ports without specifying *observe-port-index*, the system selects the smallest unused indexes and assigns the indexes to the observing ports in sequence.
- In 1:N mirroring, if you configure packets (in the inbound or outbound direction) on a mirrored port to be copied to an observing port group, the packets cannot be copied to other observing ports.
- On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, both Ethernet ports and Eth-Trunks can be configured as observing ports. On other devices, only Ethernet ports can be configured as observing ports.
- An observing port in blocked state can still forward mirrored traffic.
- You must dedicate observing ports for mirroring use and do not configure other services on them to prevent mirrored traffic and other service traffic from affecting each other. Do not configure any member port of an Eth-Trunk as an observing port. If you must do so, ensure that the bandwidth of service traffic on this port and the bandwidth occupied by the mirrored traffic do not exceed the bandwidth limit of the port. For the S6735-S, you are advised not

to modify the VLAN configuration on observing ports. Otherwise, VLAN information in the mirrored packets is incorrect.

Example

Configure GigabitEthernet0/0/1 as a local observing port.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/1
```

Configure GigabitEthernet0/0/1 through GigabitEthernet0/0/3 as a local observing port group.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface-range gigabitethernet 0/0/1 to gigabitethernet 0/0/3
```

16.9.8 observe-port (Layer 2 remote observing port)

Function

The **observe-port** command configures Layer 2 remote observing ports.

The **undo observe-port** command deletes Layer 2 remote observing ports.

By default, no Layer 2 remote observing ports are configured.

Format

Configure a single Layer 2 remote observing port:

observe-port [*observe-port-index*] **interface** *interface-type interface-number* **vlan** *vlan-id* [**truncate packet** *packet-length*]

Configure a Layer 2 remote observing port group:

observe-port [*observe-port-index*] **interface-range** { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-n> **vlan** *vlan-id* [**truncate packet** *packet-length*](Only supported by S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S; n in &<1-n> is 4 on an S6735-S, S6720-EI, and S6720S-EI and 8 on an S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S.)

observe-port *observe-port-index* **interface-range** { **add** | **delete** } *interface-type interface-number* (Only S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.)

undo observe-port *observe-port-index*

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support **truncate packet** *packet-length*.

Parameters

Parameter	Description	Value
observe-port-index	Specifies the index of an observing port.	The value is an integer. The value ranges from 1 to 8 on the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, ranges from 1 to 4 on the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, and ranges from 1 to 6 on other devices.
interface-type interface-number	Specifies the type and number of an interface.	-
add	Adds observing ports to the observing port group.	-
delete	Deletes observing ports from the observing port group.	-
vlan *vlan-id*	Specifies the Layer 2 remote mirroring VLAN.	The value is an integer in the range from 1 to 4094.
truncate	Truncates packets to be mirrored.	-
packet *packet-length*	Specifies the length of packets to be mirrorred.	The value is an integer in the range from 64 to 1023, in bytes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In Layer 2 remote mirroring, a monitoring device and the device where an observing port resides are connected through a Layer 2 network. The device where

the observing port resides adds a specified VLAN tag to mirrored packets, and then the observing port broadcasts the mirrored packets in the Layer 2 remote mirroring VLAN so that the monitoring device can receive the mirrored packets. There are two modes for configuring observing ports: configure a single observing port and configure an observing port group. Observing port group is often used in 1:N mirroring to simplify the configuration and save observing port indexes. This is because an observing port group occupies only one observing port index regardless of how many ports are configured in the group.

Precautions

- The management interface cannot be configured as an observing port.
- If you configure observing ports without specifying *observe-port-index*, the system selects the smallest unused indexes and assigns the indexes to the observing ports in sequence.
- In 1:N mirroring, if you configure packets (in the inbound or outbound direction) on a mirrored port to be copied to an observing port group, the packets cannot be copied to other observing ports.
- On the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, both Ethernet ports and Eth-Trunks can be configured as observing ports. On other devices, only Ethernet ports can be configured as observing ports.
- An observing port in blocked state can still forward mirrored traffic.
- You must dedicate observing ports for mirroring use and do not configure other services on them to prevent mirrored traffic and other service traffic from affecting each other. Do not configure any member port of an Eth-Trunk as an observing port. If you must do so, ensure that the bandwidth of service traffic on this port and the bandwidth occupied by the mirrored traffic do not exceed the bandwidth limit of the port. For the S6735-S, you are advised not to modify the VLAN configuration on observing ports. Otherwise, VLAN information in the mirrored packets is incorrect.
- An Eth-Trunk on the S6735-S, S6720-EI, and S6720S-EI can meet at most three of the following conditions simultaneously:
  - The Eth-Trunk is a Layer 2 interface, or the working mode of the Eth-Trunk is changed from Layer 3 to Layer 2 using the **portswitch** or **portswitch batch** command.
  - The Eth-Trunk is configured as a Layer 2 remote observing port using the **observe-port** command.
  - The operating mode of the spanning tree protocol is set to VBST on the switch using the **stp mode** command.
  - VBST is enabled on the Eth-Trunk using the **stp enable** command.
- The **mac-address learning disable** command must be run in the VLAN view to disable the MAC address learning function in VLANs on all the intermediate devices between the monitoring device and the observing port. Otherwise, mirrored traffic will be discarded on the intermediate devices.

Example

Configure GigabitEthernet0/0/1 as a Layer 2 remote observing port.


```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/1 vlan 10
```

Configure GigabitEthernet0/0/1 through GigabitEthernet0/0/3 as a Layer 2 remote observing port group.

```
<HUAWEI> system-view
[HUAWEI] observe-port 2 interface-range gigabitethernet 0/0/1 to gigabitethernet 0/0/3 vlan 10
```

16.9.9 observe-port dynamic-allocation enable

Function

The **observe-port dynamic-allocation enable** command enables the function of dynamically applying for observing port resources.

The **undo observe-port dynamic-allocation enable** command restores the default configuration.

By default, the function is disabled.

NOTE

This command is supported only on the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S.

Format

observe-port *observe-port-index* **dynamic-allocation enable**

undo observe-port *observe-port-index* **dynamic-allocation enable**

Parameters

Parameter	Description	Value
observe-port-index	Specifies the index of an observing port.	The value is an integer in the range from 2 to 4. The observing port with index 1 does not support the function of dynamically applying for observing port resources.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

For the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, when the same observing

port is configured for outbound mirroring and inbound mirroring and multiple mirrored ports reside on the same switch, only one copy of the same packets is mirrored to the observing port. To resolve this problem, run the **observe-port dynamic-allocation enable** command to enable the observing port to dynamically apply for hardware resources.

Precautions

- In a stack, you can also configure the mirrored ports and observing port on different member switches to prevent this problem, without the need of running this command.
- You need to run this command before running the **observe-port** [*observe-port-index*] **interface** command to create an observing port.
- After the **observe-port dynamic-allocation enable** command is configured, observing port resources are occupied only when the **port-mirroring to observe-port** command is configured on mirrored ports. If both inbound mirroring and outbound mirroring are configured on a mirrored port, one observing port resource is occupied for each direction.

Example

Enable the function of dynamically applying for observing port resources.

```
<HUAWEI> system-view
[HUAWEI] observe-port 2 dynamic-allocation enable
[HUAWEI] observe-port 2 interface gigabitethernet 0/0/1
```

16.9.10 observe-port forwarding disable

Function

The **observe-port forwarding disable** command disables an observing port from forwarding data packets.

The **undo observe-port forwarding disable** command restores the default configuration.

By default, an observing port can forward data packets.

Format

observe-port *observe-port-index* **forwarding disable**

undo observe-port *observe-port-index* **forwarding disable**

Parameters

Parameter	Description	Value
observe-port-index	Specifies the index of an observing port.	The specified observing port must exist.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You must dedicate observing ports for mirroring use and do not configure other services on them to prevent mirrored traffic and other service traffic from affecting each other. However, the observing port is still capable of forwarding data packets by default. You can run the **observe-port forwarding disable** command to disable an observing port from forwarding data packets.

Precautions

If an observing port is an Eth-Trunk interface, this function cannot be configured for this observing port.

Example

Disable the observing port with index 1 from forwarding data packets.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 forwarding disable
```

16.9.11 port-mirroring to observe-port

Function

The **port-mirroring to observe-port** command configures a mirrored port and bind it to an observing port. That is, copy packets on the mirrored port to a specified observing port.

The **undo port-mirroring** command restores the default configuration.

By default, there are no mirrored ports on the device.

Format

port-mirroring to observe-port *observe-port-index* { **both** | **inbound** | **outbound** }

undo port-mirroring [**to observe-port** *observe-port-index*] { **both** | **inbound** | **outbound** }

Parameters

Parameter	Description	Value
observe-port-index	Specifies the index of observing ports.	The specified observing port must exist.
both	Copies inbound and outbound packets on a mirrored port to observing ports.	-
inbound	Copies inbound packets on a mirrored port to observing ports.	-
outbound	Copies outbound packets on a mirrored port to observing ports.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In port mirroring, you can run the **port-mirroring to observe-port** command to copy packets that pass through a mirrored port to specified observing ports.

Prerequisites

Observing ports have been configured using the **observe-port(local observing port)** or **observe-port(Layer 2 remote observing port)** command in the system view.

Precautions

- To prevent mirrored packets from being lost, ensure that mirrored and monitoring ports have the same port type and bandwidth.
- Both physical interfaces and Eth-Trunks can be configured as mirrored ports. If an Eth-Trunk is configured as a mirrored port, its member ports cannot be configured as observing ports.
- A mirrored port can be bound to either observing ports or observing port groups.

Example

Configure port mirroring for inbound packets on GigabitEthernet0/0/1.


```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/2
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-mirroring to observe-port 1 inbound
```

16.10 Packet Capture Configuration Commands

16.10.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.10.2 capture-packet

Function

The **capture-packet** command captures service packets matching specified rules.

Format

capture-packet { **interface** *interface-type interface-number* | **acl** { *ipv4-acl* | **ipv6** *ipv6-acl* } } * [**vlan** *vlan-id* | **cvlan** *cvlan-id*] * **destination** { **file** *file-name* | **terminal** } * [**car cir** *car-value* | **time-out** *time-out-value* | **packet-num** *number* | **packet-len** *length* | { **inbound** | **outbound** }] *

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **cvlan** *cvlan-id* and **car cir** *car-value* parameters.

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **inbound** and **outbound** parameters. If the **inbound** and **outbound** parameters are not specified, the switch captures both incoming and outgoing packets on the interface. Other switch models capture only incoming packets on the interface.

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.	-

Parameter	Description	Value
acl { *ipv4-acl* | **ipv6** *ipv6-acl* }	Captures packets matching a specified ACL or ACL6. **NOTE** The specified ACL or ACL6 must exist and contain ACL rules. The destination IPv6 address should not be specified in rules of the ACL6 for the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, or S6720S-S. Otherwise, packets will fail to be captured.	• *ipv4-acl*: The value is an integer in the range from 2000 to 5999 for the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, and from 2000 to 4999 for other models. • **ipv6** *ipv6-acl*: The value is an integer in the range from 2000 to 3999.
vlan *vlan-id*	Captures packets from a specified VLAN.	The value is an integer in the range from 1 to 4094.
cvlan *cvlan-id*	Captures packets with a specified inner VLAN ID.	The value is an integer in the range from 1 to 4094.
destination	Indicates the destination to which captured packet information is sent.	-
file *file-name*	Saves captured packet information to a file. The file name extension must be **.cap**.	The value is a string of 5 to 63 characters that cannot contain the following special characters: ~ * : / \ ' " < >
terminal	Displays captured packet information on a terminal.	-
car cir *car-value*	Specifies the rate at which packets are captured.	The value is an integer in the range from 8 to 256, in kbit/s. The default value is 64 kbit/s.

Parameter	Description	Value
time-out *time-out-value*	Specifies the timeout period for packet capture. The system stops capturing packets after the specified timeout period elapses.	• When only **file** *file-name* is specified: The value is an integer in the range from 1 to 86400, in seconds. The default timeout period is 60s. • When only **terminal** is specified or both **file** *file-name* and **terminal** are specified: The value is an integer in the range from 1 to 300, in seconds. The default timeout period 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.	• When only **file** *file-name* is specified: The value is an integer in the range from 1 to 10000. The default value is 100. • When only **terminal** is specified or both **file** *file-name* and **terminal** are specified: The value is an integer in the range from 1 to 1000. The default value is 100.
packet-len *length*	Specifies the length of captured packets.	The value is an integer in the range from 20 to 64, in bytes. The default value is 64 bytes.
inbound	Captures incoming packets on the interface.	-
outbound	Captures outgoing packets on the interface.	-

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), you can configure the switch to capture service packets for analysis so that the switch can quickly identify invalid packets.

Precautions

- Currently, packets on the management interface, logical stack ports, and stack member ports cannot be captured.
- If the IP addresses of ARP packets on the control plane match the IP addresses in a basic or advanced ACL, these ARP packets can also be captured.
- The packet capture configuration is not saved in the configuration file, and becomes invalid when packet capture is complete.
- Different packet capture instances cannot be executed simultaneously. That is, a new packet capture instance can be executed only when the previous one is complete.
- The system limits the rate of captured packets. The default rate limit is 64 kbit/s. If the rate of packets exceeds the limit, some packets may be discarded.
- The device cannot capture the packets of fast ICMP reply, BFD, 802.1ag, and VBST.
- When an S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, or S6720S-S discards the packets that it cannot forward, packets may not be captured in some situations. It is recommended that you obtain packets in other ways, such as mirroring.
- For the S1720GW-E, S1720GWR-E, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5720I-SI, S5735S-H, S5736-S, and S6720S-S, the VLAN ID in the packets captured using this command is not the original VLAN ID but the VLAN ID replaced during Layer 3 forwarding. However, the packets can be forwarded normally without affecting services.
- In an SVF system, an Eth-Trunk bound to a fabric port does not support service packet capture.

Example

Capture packets on the interface GigabitEthernet0/0/1, saves them to the capture.cap file, and display them on the terminal (on a switch that supports capture of outgoing packets on an interface).

```
<HUAWEI> system-view
[HUAWEI] capture-packet interface gigabitethernet 0/0/1 destination file capture.cap terminal
[HUAWEI]
  Packet(inbound): 1
```



```
-------------------------------------------------------------
ff ff ff ff ff ff 00 00 c1 02 01 02 81 00 00 58
08 00 45 00 00 52 00 00 00 00 40 72 c8 33 58 01
01 02 58 01 01 03 00 01 02 03 04 05 06 07 08 09
0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19
-------------------------------------------------------------

Packet(outbound): 1
-------------------------------------------------------------
ff ff ff ff ff ff 00 00 c1 02 01 02 08 00 45 00
00 52 00 00 00 00 40 72 c8 33 58 01 01 02 58 01
01 03 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d
0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d
-------------------------------------------------------------

------------------packet getting report------------------
file:  flash:/capture.cap
packets getting: interface GigabitEthernet0/0/1
acl: -
vlan: -  cvlan: -
car: 64kbps timeout: 60s
packets: 100 (expected)
        1 (inbound actual) 1 (outbound actual)
length without tunnel header: 64 (expected)
-------------------------------------------------------------
```

Capture packets on the interface GigabitEthernet0/0/1, saves them to the capture.cap file, and display them on the terminal (on a switch that does not support capture of outgoing packets on an interface).

```
<HUAWEI> system-view
[HUAWEI] capture-packet interface gigabitethernet 0/0/1 destination file capture.cap terminal
[HUAWEI]
 Packet: 1
 -------------------------------------------------------------
 01 80 c2 00 00 00 00 e0 09 87 78 90 81 00 00 01
 00 69 42 42 03 00 00 03 02 7c 80 00 00 e0 09 87
 78 90 00 00 00 00 80 00 00 e0 09 87 78 90 80 23
 00 00 14 00 02 00 0f 00 00 00 40 00 72 67 31 00
 -------------------------------------------------------------
 Packet: 2

 -------------------------------------------------------------
 01 80 c2 00 00 00 00 e0 09 87 78 90 81 00 00 01
 00 69 42 42 03 00 00 03 02 7c 80 00 00 e0 09 87
 78 90 00 00 00 00 80 00 00 e0 09 87 78 90 80 23
 00 00 14 00 02 00 0f 00 00 00 40 00 72 67 31 00
 -------------------------------------------------------------

 ------------------packet getting report------------------
 file:  flash:/capture.cap
 packets getting: interface GigabitEthernet0/0/1
 acl: -
 vlan: -  cvlan: -
 car: 64kbps timeout: 60s
 packets: 100 (expected) 2 (actual)
 length without tunnel header: 64 (expected)
 -------------------------------------------------------------
```

Table 16-68 Description of the **capture-packet** command output

Item	Description
Packet(inbound): *i*	*i*th captured (incoming/outgoing) packet. • inbound: incoming packet • outbound: outgoing packet

Item	Description
file	Local path that stores captured packets. If **NULL** is displayed, captured packets are displayed to the terminal.
packets getting	• Specific interface name: Packets on this interface are captured. • global: Packets matched a specified ACL or ACL6 are captured.
acl	ACL number matched by captured packets.
acl ipv6	ACL6 number matched by captured packets.
vlan	VLAN ID of captured packets.
cvlan	Inner VLAN ID of captured packets.
car	Rate of captured packets.
timeout	Timeout period of packet capture. The system stops capturing packets after the specified timeout period elapses.
packets	• expected: number of packets expected to be captured • actual: actual number of captured packets • inbound actual: actual number of captured incoming packets • outbound actual: actual number of captured outgoing packets
length without tunnel header	Length of captured packets, excluding the length of tunnel headers.

16.10.3 capture-packet cpu

Function

The **capture-packet cpu** command captures packets sent to the CPU.

Format

capture-packet cpu [**vlan** *vlan-id* | **acl** { *ipv4-acl* | **ipv6** *ipv6-acl* }] * **destination** { **file** *file-name* | **terminal** } * [**time-out** *time-out-value* | **packet-num** *number* | **packet-len** *length*] *

Parameters

Parameter	Description	Value
vlan *vlan-id*	Captures packets from a specified VLAN.	The value is an integer that ranges from 1 to 4094.
acl { *ipv4-acl* | **ipv6** *ipv6-acl* }	Captures packets matching a specified ACL or ACL6. **NOTE** The specified ACL or ACL6 must exist and contain ACL rules. The destination IPv6 address should not be specified in rules of the ACL6 for the S1720GW-E, S1720GWR-E, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, or S6720S-S. Otherwise, packets will fail to be captured.	• *ipv4-acl*: The value is an integer in the range from 2000 to 5999 for the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S, and from 2000 to 4999 for other models. • **ipv6** *ipv6-acl*: The value is an integer in the range from 2000 to 3999.
destination	Indicates the destination to which captured packet information is sent.	-
file *file-name*	Saves captured packet information to a file. The file name extension must be **.cap**.	The value is a string of 5 to 63 characters that cannot contain the following special characters: ~ * : / \ ' " < >
terminal	Displays captured packet information on a terminal.	-

Parameter	Description	Value
time-out *time-out-value*	Specifies the timeout period for packet capture. The system stops capturing packets after the specified timeout period elapses.	• When only **file** *file-name* is specified: The value is an integer in the range from 1 to 86400, in seconds. The default timeout period is 60s. • When only **terminal** is specified or both **file** *file-name* and **terminal** are specified: The value is an integer in the range from 1 to 300, in seconds. The default timeout period 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.	• When only **file** *file-name* is specified: The value is an integer in the range from 1 to 10000. The default value is 100. • When only **terminal** is specified or both **file** *file-name* and **terminal** are specified: The value is an integer in the range from 1 to 1000. The default value is 100.
packet-len *length*	Specifies the length of captured packets.	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 a CPU fault occurs (for example, the CPU usage is high), configure the packet capture function to capture packets sent to the CPU for analysis. This allows the switch to process invalid packets promptly, ensuring that the CPU works properly.

Precautions

- If the IP addresses of ARP packets on the control plane match the IP addresses in a basic or advanced ACL, these ARP packets can also be captured.
- Running this command will increase the CPU usage. Therefore, you are not advised to run this command if the CPU usage is higher than the specified value in a Warning message.
- The packet capture configuration is not saved in the configuration file, and becomes invalid when packet capture is complete.
- Different packet capture instances cannot be executed simultaneously. That is, a new packet capture instance can be executed only when the previous one is complete.
- The system limits the rate of captured packets. The default rate limit is 64 kbit/s. If the rate of packets exceeds the limit, some packets may be discarded.

Example

Capture the packets to be sent to the CPU, save them to the **abc.cap** file, and display them on the terminal.

```
<HUAWEI> system-view
[HUAWEI] capture-packet cpu destination file flash:/abc.cap
[HUAWEI]
  Packet: 1
  ------------------------------------------------------------
  01 80 c2 00 00 0e 00 e0 09 87 78 90 81 00 00 01
  88 cc 02 07 04 00 e0 09 87 78 90 04 16 05 47 69
  67 61 62 69 74 45 74 68 65 72 6e 65 74 34 2f 30
  2f 32 36 06 02 00 78 08 15 47 69 67 61 62 69 74
  ------------------------------------------------------------

  Packet: 2
  ------------------------------------------------------------
  01 80 c2 00 00 0e 00 e0 09 87 78 90 81 00 00 01
  88 cc 02 07 04 00 e0 09 87 78 90 04 16 05 47 69
  67 61 62 69 74 45 74 68 65 72 6e 65 74 34 2f 30
  2f 32 36 06 02 00 78 08 15 47 69 67 61 62 69 74
  ------------------------------------------------------------

  ------------------packet getting report-----------------------
  file: flash:/abc.cap
  packets getting: cpu
  acl: -
  vlan: -  cvlan: -
  car: -- timeout: 60s
  packets: 100 (expected) 2 (actual)
  length without tunnel header: 64 (expected)
  ------------------------------------------------------------
```

Table 16-69 Description of the **capture-packet cpu** command output

Item	Description
Packet: *i*	*i*th captured packet.

Item	Description
file	Local path that stores captured packets. If **NULL** is displayed, captured packets are displayed on a terminal, instead of being saved to a specified file.
packets getting	The system captures the packets to be sent to the CPU.
acl	ACL number matched by captured packets.
acl ipv6	ACL6 number matched by captured packets.
vlan	VLAN ID of captured packets.
cvlan	Inner VLAN ID of captured packets.
car	Rate of captured packets.
timeout	Timeout period of packet capture. The system stops capturing packets after the specified timeout period elapses.
packets	• expected: number of packets expected to be captured • actual: actual number of captured packets
length without tunnel header	Length of captured packets, excluding the length of tunnel headers.

16.10.4 capture-packet stop

Function

The **capture-packet stop** command stops capturing service packets.

Format

capture-packet stop

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If you need to update service packet capture parameters or no longer need to capture service packets after running the **capture-packet** command, you can run the **capture-packet stop** command to stop capturing service packets.

Example

Stop capturing service packets.

```
<HUAWEI> system-view
[HUAWEI] capture-packet stop
```

16.11 NetStream Configuration Commands

NOTE

NetStream collects statistics and analyzes service traffic. During service provisioning, personal data may be involved. You have an obligation to make privacy policies and take measures according to the applicable law of the country to protect personal data.

16.11.1 Command Support

Only the following switch models support NetStream:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S

16.11.2 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.	-

Parameter	Description	Value
packets	Indicates that the flexible flow statistics exported to NSC contain the number of packets.	-

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 contain the number of bytes and packets.

Precaution

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.

The command can be run multiple times, and all the configurations take effect.

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
```

16.11.3 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** }

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.

Precaution

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.

The command can be run multiple times, and all the configurations take effect.

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
```


16.11.4 collect ip bgp-next-hop

Function

The **collect ip bgp-next-hop** command configures the flexible flow statistics exported to the NSC to contain the BGP next hop information of a flow.

The **undo collect ip bgp-next-hop** command restores the default setting.

By default, the flexible flow statistics exported to the NSC do not contain the BGP next hop information of a flow.

Format

collect ip bgp-next-hop

undo collect ip bgp-next-hop

Parameters

None

Views

Flexible flow statistics template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain richer flow statistics, configure whether the flexible flow statistics exported to the NSC contain the BGP next hop information of a flow.

To enable the flexible flow statistics sent to the NSC to contain the BGP next hop information, you also need to run the **collect ip bgp-next-hop** and **ip netstream export version 9 bgp-nexthop** commands.

Precautions

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.

Example

Configure the flexible flow statistics exported to the NSC to contain the BGP next hop information of a flow.

```
<HUAWEI> system-view
[HUAWEI] ip netstream record record1
[HUAWEI-record-record1] collect ip bgp-next-hop
```


16.11.5 collect ip next-hop

Function

The **collect ip next-hop** command configures the flexible flow statistics exported to the NSC to contain the next hop information of a flow.

The **undo collect ip next-hop** command restores the default setting.

By default, the flexible flow statistics exported to the NSC do not contain the next hop information of a flow.

Format

collect ip next-hop

undo collect ip next-hop

Parameters

None

Views

Flexible flow statistics template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain richer flow statistics, configure whether the flexible flow statistics exported to the NSC contain the next hop information of a flow.

Precautions

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.

Example

Configure the flexible flow statistics exported to the NSC to contain the next hop information of a flow.

```
<HUAWEI> system-view
[HUAWEI] ip netstream record record1
[HUAWEI-record-record1] collect ip next-hop
```


16.11.6 collect ip tcp-flag

Function

The **collect ip tcp-flag** command configures the flexible flow statistics exported to the NSC to contain the TCP flags of a flow.

The **undo collect ip tcp-flag** command restores the default setting.

By default, the flexible flow statistics exported to the NSC do not contain the TCP flags of a flow.

Format

collect ip tcp-flag

undo collect ip tcp-flag

Parameters

None

Views

Flexible flow statistics template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain richer flow statistics, configure whether the flexible flow statistics exported to the NSC contain the TCP flags of a flow.

Precautions

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.

Example

Configure the flexible flow statistics exported to the NSC to contain the TCP flags of a flow.

```
<HUAWEI> system-view
[HUAWEI] ip netstream record record1
[HUAWEI-record-record1] collect ip tcp-flag
```


16.11.7 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* } [**vxlan inner-ip**]

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*.	The flexible flow statistics template must be existed.
vxlan inner-ip	Displays configurations of VXLAN flexible flow statistics templates.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

After you create and configure a flexible flow statistics template using the **ip netstream record** command, you can run the **display ip netstream record** command to view the configuration of the template.

Example

Display the configuration of the flexible flow statistics template **test0**.

```
<HUAWEI> display ip netstream record name test0
ip netstream record test0
 match ip source-address
 match ip destination-address
 match vlan input
```


Table 16-70 Description of the **display ip netstream record** command output

Item	Description
ip netstream record *record-name*	The flexible flow statistics template is *record-name*. You can run the **ip netstream record** command to configure this parameter.
match *x*	This template aggregates packets based on *x*. For the meaning and configuration of *x*, see the **match** command in the flexible flow statistics template view.

16.11.8 display ip netstream statistics

Function

The **display ip netstream statistics** command displays the NetStream flow statistics.

Format

display ip netstream statistics slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a slot ID.	The value depends on the actual configuration.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After NetStream is configured, you can run the **display ip netstream statistics** command to view NetStream statistics.

Precautions

After each statistics item in the command output reaches the maximum value, it is reset to 0. To ensure accurate statistics about NetStream flows, you are advised to run the **reset ip netstream statistics** command to clear statistics about current NetStream flows before running the **display ip netstream statistics** command.

Example

Display the NetStream flow statistics on the device.

```
<HUAWEI> display ip netstream statistics slot 0
 =====Netstream statistics:=====
 Origin/Flexible ingress entries  : 572
 Origin/Flexible ingress packets  : 56122
 Origin/Flexible ingress octets   : 6762976
 Origin/Flexible egress entries   : 57
 Origin/Flexible egress packets   : 3588
 Origin/Flexible egress octets    : 394680
 Origin/Flexible total entries    : 629
 Handle origin entries            : 620
 Handle As aggre entries          : 12
 Handle ProtPort aggre entries    : 11
 Handle SrcPrefix aggre entries   : 10
 Handle DstPrefix aggre entries   : 15
 Handle Prefix aggre entries      : 7
 Handle AsTos aggre entries       : 6
 Handle ProtPortTos aggre entries : 5
 Handle SrcPreTos aggre entries   : 5
 Handle DstPreTos aggre entries   : 4
 Handle PreTos aggre entries      : 1
 Record test handle entries : 0
 VXLAN-Record test handle entries : 0
```

Table 16-71 Description of the **display ip netstream statistics** command output

Item	Description
Netstream statistics	NetStream statistics.
Origin/Flexible ingress entries	Total number of incoming original flows or flexible flows.
Origin/Flexible ingress packets	Total number of packets in incoming original flows or flexible flows.
Origin/Flexible ingress octets	Total number of bytes in incoming original flows or flexible flows.
Origin/Flexible egress entries	Total number of outgoing original flows or flexible flows.
Origin/Flexible egress packets	Total number of packets in outgoing original flows or flexible flows.
Origin/Flexible egress octets	Total number of bytes in outgoing original flows or flexible flows.
Origin/Flexible total entries	Total number of original flows or flexible flows of the real-time statistics.
Handle origin entries	Number of processed incoming and outgoing original 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.

Item	Description
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.
Record test handle entries	Number of flows processed using the flexible flow statistics template **test**.
VXLAN-Record test handle entries	Number of flows processed using the VXLAN flexible flow statistics template **test**.

16.11.9 display netstream

Function

The **display netstream** command displays the NetStream configurations.

Format

display netstream { **all** | **global** | **interface** *interface-type interface-number* }

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 template view • NetStream configurations in the interface view	-
global	Displays the global NetStream configurations, including: • NetStream configurations in the system view • NetStream configurations in the aggregation view • NetStream configurations in the flexible flow statistics template view	-
interface *interface-type interface-number*	Displays the NetStream configurations on a specified interface. The parameter *interface-type interface-number* specifies the interface type and number.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

This command displays the NetStream configurations for both IPv4 and IPv6 flows.

Example

Display all the NetStream configurations.

```
<HUAWEI> display netstream all
system
ip netstream export version 9
ip netstream export source 10.1.1.1
ip netstream export host 10.0.0.2 6000 vpn-instance test
ip netstream export host 10.5.5.5 6000
ipv6 netstream export version 9
ipv6 netstream export host 10.0.0.3 6000 vpn-instance test12
ip netstream record test
ip netstream record test1 vxlan inner-ip
ip netstream aggregation destination-prefix
 enable
 export version 9
ip netstream aggregation protocol-port
 export version 9

slot 0
GigabitEthernet0/0/1
 ip netstream inbound
```

Table 16-72 Description of the **display netstream all** command output

Item	Description
system	Global NetStream configurations.
ip netstream export version *version*	The field *version* indicates the version of the exported packets carrying IPv4 original flow statistics. This field is displayed only when the **ip netstream export version** command has been executed. If the version retains the default setting, this field is not displayed.
ip netstream export host *ip-address port-number* vpn-instance *vpn-instance-name*	The *ip-address* field indicates the destination address of the exported packets carrying IPv4 flow statistics. The *port-number* field is the UDP port. The *vpn-instance-name* field is the name of the VPN instance to which the specified destination address belongs. This field is displayed only when the **ip netstream export host** command has been executed in the system view.
ip netstream export source *ip-address*	The field *ip-address* indicates the source address of the exported packets carrying IPv4 flow statistics. This field is displayed only when the **ip netstream export source** command has been executed. If the source address is not specified, the outbound interface IP address is used.

Item	Description
ipv6 netstream export version *version*	The field *version* indicates the version of the exported packets carrying IPv6 original flow statistics. This field is displayed only when the **ipv6 netstream export version** command has been executed. If the version retains the default setting, this field is not displayed.
ipv6 netstream export host *ip-address port-number* vpn-instance *vpn-instance-name*	The *ip-address* field indicates the destination address of the exported packets carrying IPv6 flow statistics. The *port-number* field is the UDP port. The *vpn-instance-name* field is the name of the VPN instance to which the specified destination address belongs. This field is displayed only when the **ipv6 netstream export host** command has been executed in the system view.
ip netstream record *record-name*	The flexible flow statistics template is *record-name*. This field is displayed only when the **ip netstream record** command has been executed in the system view. If the flexible flow statistics template is not specified, this field is not displayed.
ip netstream record *record-name* vxlan inner-ip	The VXLAN flexible flow statistics template is *record-name*. This field is displayed only when the **ip netstream record** command has been executed in the system view.

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 methods 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 method 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.
slot *x*	NetStream configurations on the card in slot *x*.
GigabitEthernet0/0/1 ip netstream inbound	The flow statistics function is enabled for incoming packets on GigabitEthernet0/0/1. This field is displayed only when the **ip netstream** command has been executed in the interface view.

16.11.10 display netstream cache ip aggregation

Function

The **display netstream cache ip aggregation** command displays details about IPv4 aggregation flow statistics on a device.

Format

display netstream cache ip aggregation { **as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** } **slot** *slot-id*

Parameters

Parameter	Description	Value
as	Specifies the AS aggregation. It classifies flows based on source AS number, destination AS number, inbound interface index, and outbound interface index.	-
as-tos	Specifies the AS-ToS aggregation. It classifies flows based on source AS number, destination AS number, inbound interface index, outbound interface index, and ToS.	-
destination-prefix	Specifies the destination-prefix aggregation. It classifies flows based on destination AS number, destination mask length, destination prefix, and outbound interface index.	-
destination-prefix-tos	Specifies the destination-prefix-ToS aggregation. It classifies flows based on destination AS number, destination mask length, destination prefix, outbound interface index, and ToS.	-
prefix	Specifies the prefix aggregation. It classifies flows based on source AS number, destination AS number, source mask length, destination mask length, source prefix, destination prefix, inbound interface index, and outbound interface index.	-
prefix-tos	Specifies the prefix-ToS aggregation. It classifies flows based on source AS number, destination AS number, source mask length, destination mask length, source prefix, destination prefix, inbound interface index, outbound interface index, and ToS.	-
protocol-port	Specifies the protocol-port aggregation. It classifies flows based on protocol number, source port, and destination port.	-
protocol-port-tos	Specifies the protocol-port-ToS aggregation. It classifies flows based on protocol number, source port, destination port, ToS, inbound interface index, and outbound interface index.	-

Parameter	Description	Value
source-prefix	Specifies the source-prefix aggregation. It classifies flows based on source AS number, source mask length, source prefix, and 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, and inbound interface index.	-
slot *slot-id*	Specifies the slot ID.	The value depends on the device configuration.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command displays real-time statistics on IPv4 aggregation flows on the device.

Precaution

This command must be executed before the flows age out; otherwise, no information will be displayed.

Example

Display detailed statistics about flows aggregated based on protocol and port on the device.

```
<HUAWEI> display netstream cache ip aggregation protocol-port slot 0
NetStream cache information:
------------------------------------------------------------------------------
 Protocol   SrcPort   DstPort   Direction  Streams     Packets     Octets
------------------------------------------------------------------------------
 114        0         0         IN         200         50688       5271552
------------------------------------------------------------------------------
.............
```


Table 16-73 Description of the **display netstream cache ip aggregation** command output

Item	Description
NetStream cache information	NetStream flow information.
Protocol	Protocol number of packets.
SrcPort	Source port number of packets.
DstPort	Destination port number of packets.
Direction	Packet sampling direction: • IN: inbound direction • OUT: outbound direction
Streams	Number of flows.
Packets	Number of packets.
Octets	Number of octets in packets.

16.11.11 display netstream cache ip record

Function

The **display netstream cache ip record** command displays details about IPv4 flexible flow statistics on a device.

Format

display netstream cache ip record *record-name* [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination ip** *ip-address* | **destination port** *port-number* | **destination mac-address** *mac-address* | **source interface** *interface-type interface-number* | **source ip** *ip-address* | **source port** *port-number* | **source mac-address** *mac-address* | **protocol** *protocol-type* | **tos** *tos-number* | **ttl** *ttl-number* | **vlan** *vlan-id*] * **slot** *slot-id* [**verbose**]

NOTE

If the **destination mac-address** *mac-address*, **source mac-address** *mac-address*, **ttl** *ttl-number*, or **vlan** *vlan-id* parameter is specified, the **verbose** parameter must be specified too.

Parameters

Parameter	Description	Value
record-name	Specifies the name of a flexible flow statistics template.	It must be an existing template name on the device.

Parameter	Description	Value
inbound	Specifies incoming packets.	-
outbound	Specifies outgoing packets.	-
destination interface *interface-type interface-number*	Specifies the destination interface of packets.	-
destination ip *ip-address*	Specifies the destination IP address of packets.	-
destination port *port-number*	Specifies the destination port number of packets.	The value is an integer that ranges from 0 to 65535.
destination mac-address *mac-address*	Specifies the destination MAC address of packets.	-
source interface *interface-type interface-number*	Specifies the source interface of packets.	-
source ip *ip-address*	Indicates the source IP address of packets.	-
source port *port-number*	Specifies the source port number of packets.	The value is an integer that ranges from 0 to 65535.
source mac-address *mac-address*	Specifies the source MAC address of packets.	-
protocol *protocol-type*	Specifies the protocol type of packets.	The value is an integer that ranges from 0 to 255.
tos *tos-number*	Specifies the ToS value of packets.	The value is an integer that ranges from 0 to 255.
ttl *ttl-number*	Specifies the TTL value of packets.	The value is an integer that ranges from 1 to 255.
vlan *vlan-id*	Specifies the VLAN ID of packets.	The value is an integer that ranges from 1 to 4094.
slot *slot-id*	Specifies the slot ID.	The value depends on the device configuration.
verbose	Displays detailed information.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command displays real-time statistics on IPv4 flexible flows on the device.

Precaution

This command must be executed before the flows age out; otherwise, no information will be displayed.

Example

Display IPv4 flexible flow statistics on the device.

```
<HUAWEI> display netstream cache ip record record1 slot 0 verbose
NOTE:    L4 Info: Source Port:Destination Port:Protocol
         TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent
NetStream cache information:
------------------------------------------------------------------------------
 SrcIP              DstIP             L4 Info           DstAS     Direction
 SrcIf              DstIf             TCP Flags         SrcAS     ToS
 NextHop            BGPNextHop        Octets            Packets   TTL
 SMAC               DMAC              VLAN
------------------------------------------------------------------------------
 255.255.255.255    255.255.255.255   0:0:0             100       OUT
 GE0/0/10           GE0/0/11          0:0:0:0:0:0       --        0
 10.1.1.1           10.1.1.1          528               4         20
 00:e0:fc:12:23:56  00:e0:fc:12:23:33 60
------------------------------------------------------------------------------
```

Table 16-74 Description of the **display netstream cache ip record** command output

Item	Description
NOTE	Note.
L4 Info: Source Port:Destination Port:Protocol	Transport-layer information of packets, including source port, destination port, and protocol type.
TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent	TCP flag of packets, including ACK, Fin, Push, Reset, Syn, and Urgent.
NetStream cache information	NetStream flow information.

Item	Description
SrcIP	Source IP address of packets.
DstIP	Destination IP address of packets.
DstAS	Destination AS number of packets.
Direction	Packet sampling direction: • IN: inbound direction. • OUT: outbound direction.
SrcIf	Source interface of packets.
DstIf	Destination interface of packets.
SrcAS	Source AS number of packets.
ToS	ToS field of packets.
NextHop	Next hop address.
BGPNextHop	Address of the BGP next hop.
Octets	Number of octets in packets.
Packets	Number of packets.
TTL	TTL value of packets.
SMAC	Source MAC address of packets.
DMAC	Destination MAC address of packets.
VLAN	VLAN ID of packets.

16.11.12 display netstream cache vxlan record

Function

The **display netstream cache vxlan record** command displays detailed VXLAN flexible flow statistics.

Format

display netstream cache vxlan inner-ip [ipv6] record *record-name* [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination ip** *ip-address* | **destination port** *port-number* | **destination mac-address** *mac-address* | **source interface** *interface-type interface-number* | **source ip** *ip-address* | **source port** *port-number* | **source mac-address** *mac-address* | **protocol** *protocol-type* | **tos** *tos-number* | **ttl** *ttl-number* | **vlan** *vlan-id*] * **slot** *slot-id* [**verbose**]

NOTE

When **destination mac-address** *mac-address*, **source mac-address** *mac-address*, **ttl** *ttl-number*, or **vlan** *vlan-id* is specified, the **verbose** parameter must also be specified.

Parameters

Parameter	Description	Value
ipv6	Displays detailed IPv6 information about VXLAN flexible flows. If this parameter is not specified, detailed IPv4 information about VXLAN flexible flows is displayed by default.	-
record-name	Specifies the name of a flexible flow statistics template.	It must be an existing template name on the switch.
inbound	Specifies incoming packets.	-
outbound	Specifies outgoing packets.	-
destination interface *interface-type interface-number*	Specifies the destination interface of packets.	-
destination ip *ip-address*	Specifies the destination IP address of packets.	-
destination port *port-number*	Specifies the destination port number of packets.	The value is an integer in the range 0 to 65535.
destination mac-address *mac-address*	Specifies the destination MAC address of packets.	-
source interface *interface-type interface-number*	Specifies the source interface of packets.	-
source ip *ip-address*	Specifies the source IP address of packets.	-
source port *port-number*	Specifies the source port number of packets.	The value is an integer in the range 0 to 65535.
source mac-address *mac-address*	Specifies the source MAC address of packets.	-
protocol *protocol-type*	Specifies the packet protocol type.	The value is an integer in the range from 0 to 255.

Parameter	Description	Value
tos *tos-number*	Specifies the ToS value of packets.	The value is an integer in the range from 0 to 255.
ttl *ttl-number*	Specifies the TTL value of packets.	The value is an integer in the range from 1 to 255.
vlan *vlan-id*	Indicates the VLAN ID of packets.	The value is an integer in the range from 1 to 4094.
slot *slot-id*	Specifies a slot ID.	The value depends on the actual configuration.
verbose	Displays detailed information.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command displays detailed real-time VXLAN flexible flow statistics.

Precautions

This command must be executed before the flows age out; otherwise, no information will be displayed.

Example

Display detailed IPv4 information about VXLAN flexible flows on the switch.

```
<HUAWEI> display netstream cache vxlan inner-ip record record1 slot 0 verbose
NOTE:    L4 Info: Source Port:Destination Port:Protocol
         TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent
NetStream cache information:
------------------------------------------------------------------------------
 SrcIP               DstIP             L4 Info           DstAS     Direction
 SrcIf               DstIf             TCP Flags         SrcAS     ToS
 NextHop             BGPNextHop        Octets            Packets   TTL
 SMAC                DMAC              VLAN              VNI
------------------------------------------------------------------------------
 255.255.255.255     255.255.255.255   0:0:0             100       OUT
 GE0/0/10            GE0/0/11          0:0:0:0:0:0       --        0
 10.1.1.1            10.1.1.1          528               4         20
 00:e0:fc:12:23:56   00:e0:fc:12:23:33 60
------------------------------------------------------------------------------
```


Table 16-75 Description of the **display netstream cache vxlan record** command output

Item	Description
NOTE	Note.
L4 Info: Source Port:Destination Port:Protocol	Transport-layer information of packets, including the source port number, destination port number, and protocol type.
TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent	TCP flag of a packet, including ACK, Fin, Push, Reset, Syn, and Urgent.
NetStream cache information	NetStream flow information.
SrcIP	Source IP address of packets.
DstIP	Destination IP address of packets.
DstAS	Destination AS number of packets.
Direction	Packet sampling direction: • IN: inbound direction • OUT: outbound direction
SrcIf	Source interface of packets.
DstIf	Destination interface of packets.
SrcAS	Source AS number of packets.
ToS	ToS value of packets.
NextHop	Next-hop IP address in a route.
BGPNextHop	IP address of the BGP next hop.
Octets	Number of octets in packets.
Packets	Number of packets.
TTL	TTL value of packets.
SMAC	Source MAC address of packets.
DMAC	Destination MAC address of packets.
VLAN	VLAN ID of packets.
VNI	VNI ID of packets.

16.11.13 display netstream cache ip origin

Function

The **display netstream cache ip origin** command displays details about IPv4 original flow statistics on a device.

Format

display netstream cache ip origin [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination ip** *ip-address* | **destination port** *port-number* | **source interface** *interface-type interface-number* | **source ip** *ip-address* | **source port** *port-number* | **protocol** *protocol-type* | **tos** *tos-number*] * **slot** *slot-id* [**verbose**]

Parameters

Parameter	Description	Value
inbound	Specifies incoming packets.	-
outbound	Specifies outgoing packets.	-
destination interface *interface-type interface-number*	Specifies the destination interface of packets.	-
destination ip *ip-address*	Specifies the destination IP address of packets.	-
destination port *port-number*	Specifies the destination port number of packets.	The value is an integer that ranges from 0 to 65535.
source interface *interface-type interface-number*	Specifies the source interface of packets.	-
source ip *ip-address*	Indicates the source IP address of packets.	-
source port *port-number*	Specifies the source port number of packets.	The value is an integer that ranges from 0 to 65535.
protocol *protocol-type*	Specifies the protocol type of packets.	The value is an integer that ranges from 0 to 255.
tos *tos-number*	Specifies the ToS value of packets.	The value is an integer that ranges from 0 to 255.

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value depends on the device configuration.
verbose	Displays detailed information.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command displays real-time statistics on IPv4 original flows on the device.

Precaution

This command must be executed before the flows age out; otherwise, no information will be displayed.

Example

Display details about IPv4 original flow statistics on the device.

```
<HUAWEI> display netstream cache ip origin slot 0 verbose
NOTE:    L4 Info: Source Port:Destination Port:Protocol
         TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent
NetStream cache information:
------------------------------------------------------------------------------
 SrcIf             SrcIP/Mask          DstIP/Mask          L4 Info
 ToS               Direction           SrcAS               DstAS
 DstIf             TCP Flags           Octets              Packets
 NextHop           BGPNextHop
------------------------------------------------------------------------------
 GE0/0/5           10.1.1.2/--         10.1.1.1/--         0:0:114
 0                 IN                  --                  --
 --                0:0:0:0:0:0         5200                50
 --                --
------------------------------------------------------------------------------
.....................
```

Table 16-76 Description of the **display netstream cache ip origin** command output

Item	Description
NOTE	Note.

Item	Description
L4 Info: Source Port:Destination Port:Protocol	Transport-layer information of packets: including source port, destination port, and protocol type.
TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent	TCP flag of packets: including ACK, Fin, Push, Reset, Syn, and Urgent.
NetStream cache information	NetStream flow information.
SrcIf	Source interface of packets.
SrcIP/Mask	Source IP address and mask of packets.
DstIP/Mask	Destination IP address and mask of packets.
ToS	ToS of packets.
Direction	Packet sampling direction: • IN: inbound direction • OUT: outbound direction
SrcAS	Source AS number of packets.
DstAS	Destination AS number of packets.
DstIf	Destination interface of packets.
Octets	Number of octets in packets.
Packets	Number of packets.
NextHop	Next hop address.
BGP NextHop	BGP next hop address.

16.11.14 display netstream cache ipv6 record

Function

The **display netstream cache ipv6 record** command displays details about IPv6 flexible flow statistics on a device.

Format

display netstream cache ipv6 record *record-name* [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination ipv6** *ipv6-address* | **destination port** *port-number* | **destination mac-address** *mac-address* | **source interface** *interface-type interface-number* | **source ipv6** *ipv6-address* | **source port** *port-number* | **source mac-address** *mac-address* | **flowlabel** *flowlabel* | **protocol** *protocol-type* | **tos** *tos-number* | **ttl** *ttl-number* | **vlan** *vlan-id*] * **slot** *slot-id* [**verbose**]

Parameters

Parameter	Description	Value
record-name	Specifies the name of a flexible flow statistics template.	It must be an existing template name on the device.
inbound	Specifies incoming packets.	-
outbound	Specifies outgoing packets.	-
destination interface *interface-type interface-number*	Specifies the destination interface of packets.	-
destination ipv6 *ipv6-address*	Specifies the destination IPv6 address of packets.	-
destination port *port-number*	Specifies the destination port number of packets.	The value is an integer that ranges from 0 to 65535.
destination mac-address *mac-address*	Specifies the destination MAC address of packets.	-
source interface *interface-type interface-number*	Specifies the source interface of packets.	-
source ipv6 *ipv6-address*	Specifies the source IPv6 address of packets.	-
source port *port-number*	Specifies the source port number of packets.	The value is an integer that ranges from 0 to 65535.
source mac-address *mac-address*	Specifies the source MAC address of packets.	-
flowlabel *flowlabel*	Specifies the flow label of packets.	The value is an integer that ranges from 0 to 1048575.
protocol *protocol-type*	Specifies the protocol type of packets.	The value is an integer that ranges from 0 to 255.
tos *tos-number*	Specifies the ToS value of packets.	The value is an integer that ranges from 0 to 255.
ttl *ttl-number*	Specifies the TTL value of packets.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
vlan *vlan-id*	Specifies the VLAN ID of packets.	The value is an integer that ranges from 1 to 4094.
slot *slot-id*	Specifies the slot ID.	The value depends on the device configuration.
verbose	Displays detailed information.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command displays real-time statistics on IPv6 flexible flows on the device.

Precaution

This command must be executed before the flows age out; otherwise, no information will be displayed.

Example

Display IPv6 flexible flow statistics on the device.

```
<HUAWEI> display netstream cache ipv6 record test slot 0 verbose
NOTE:    L4 Info: Source Port:Destination Port:Protocol
       TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent
NetStream cache information:
------------------------------------------------------------------------------
 SrcIP                          SrcIf              L4 Info
 DstIP                          DstIf              ToS
 NextHop                          SrcAS              DstAS
 BGPNextHop                         FlowLabel          Direction
 TCP Flags                        Octets             Packets
 SMAC                             VLAN               TTL
 DMAC
------------------------------------------------------------------------------
 FC00:1::2                        GE0/0/10           0:0:0
 FC00:3::2                        GE0/0/11           0
 FC00:2::2                        --                 --
 FC00:2::2                            0                  OUT
 0:0:0:0:0:0                      6204               47
 00:e0:fc:12:34:56                  60                 20
 00:e0:fc:12:34:78
------------------------------------------------------------------------------
```


Table 16-77 Description of the **display netstream cache ipv6 record** command output

Item	Description
NOTE	Note.
L4 Info: Source Port:Destination Port:Protocol	Transport-layer information of packets, including source port, destination port, and protocol type.
TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent	TCP flag of packets, including ACK, Fin, Push, Reset, Syn, and Urgent.
NetStream cache information	NetStream flow information.
SrcIP	Source IPv6 address of packets.
SrcIf	Source interface of packets.
DstIP	Destination IPv6 address of packets.
DstIf	Destination interface of packets.
ToS	ToS of packets.
NextHop	Next hop address.
SrcAS	Source AS number of packets.
DstAS	Destination AS number of packets.
BGPNextHop	Address of the BGP next hop.
FlowLabel	IPv6 flow label.
Direction	Packet sampling direction: • IN: inbound direction. • OUT: outbound direction.
Octets	Number of octets in packets.
Packets	Number of packets.
SMAC	Source MAC address of packets.
VLAN	VLAN ID of packets.
TTL	TTL value of packets.
DMAC	Destination MAC address of packets.

16.11.15 display netstream cache ipv6 origin

Function

The **display netstream cache ipv6 origin** command displays details about IPv6 original flow statistics on a device.

Format

display netstream cache ipv6 origin [{ **inbound** | **outbound** } | **destination interface** *interface-type interface-number* | **destination ipv6** *ipv6-address* | **destination port** *port-number* | **source interface** *interface-type interface-number* | **source ipv6** *ipv6-address* | **source port** *port-number* | **flowlabel** *flowlabel* | **protocol** *protocol-type* | **tos** *tos-number*] * **slot** *slot-id* [**verbose**]

Parameters

Parameter	Description	Value
inbound	Specifies incoming packets.	-
outbound	Specifies outgoing packets.	-
destination interface *interface-type interface-number*	Specifies the destination interface of packets.	-
destination ipv6 *ipv6-address*	Specifies the destination IPv6 address of packets.	-
destination port *port-number*	Specifies the destination port number of packets.	The value is an integer that ranges from 0 to 65535.
source interface *interface-type interface-number*	Specifies the source interface of packets.	-
source ipv6 *ipv6-address*	Specifies the source IPv6 address of packets.	-
source port *port-number*	Specifies the source port number of packets.	The value is an integer that ranges from 0 to 65535.
flowlabel *flowlabel*	Specifies the flow label of packets.	The value is an integer that ranges from 0 to 1048575.
protocol *protocol-type*	Specifies the protocol type of packets.	The value is an integer that ranges from 0 to 255.

Parameter	Description	Value
tos *tos-number*	Specifies the ToS value of packets.	The value is an integer that ranges from 0 to 255.
slot *slot-id*	Specifies the slot ID.	The value depends on the device configuration.
verbose	Displays detailed information.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command displays real-time statistics on IPv6 original flows on the device.

Precaution

This command must be executed before the flows age out; otherwise, no information will be displayed.

Example

Display details about IPv6 original flow statistics on the device.

```
<HUAWEI> display netstream cache ipv6 origin slot 0 verbose
NOTE:    L4 Info: Source Port:Destination Port:Protocol
         TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent
NetStream cache information:
------------------------------------------------------------------------------
 SrcIf             TCP Flags        SrcIP/Mask
 DstIf             ToS              DstIP/Mask
 L4 Info           FlowLable        NextHop
 SrcAS             DstAS            BGP NextHop
 Direction         Octets           Packets
------------------------------------------------------------------------------
 GE0/0/5           0:0:0:0:0:0      FEC0::801:200:0:A01:102/--
 --                0                FEC0::801:200:0:C108:101/--
 0:0:59            0                --
 --                --               --
 IN                3821896          36749
------------------------------------------------------------------------------
.....................
```


Table 16-78 Description of the **display netstream cache ipv6 origin** command output

Item	Description
NOTE	Note.
L4 Info: Source Port:Destination Port:Protocol	Transport-layer information of packets: including source port, destination port, and protocol type.
TCP Flags: Ack, Fin, Push, Reset, Syn, Urgent	TCP flag of packets: including ACK, Fin, Push, Reset, Syn, and Urgent.
NetStream cache information	NetStream flow information.
SrcIf	Source interface of packets.
SrcIP/Mask	Source IPv6 address and mask of packets.
DstIf	Destination interface of packets.
ToS	Service type of packets.
DstIP/Mask	Destination IPv6 address and mask of packets.
FlowLable	IPv6 flow label.
NextHop	Next hop address.
SrcAS	Source AS number of packets.
DstAS	Destination AS number of packets.
BGP NextHop	BGP next hop address.
Direction	Packet sampling direction: • IN: inbound direction • OUT: outbound direction
Octets	Number of octets in packets.
Packets	Number of packets.

16.11.16 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

Default Level

3: Management level

Usage Guidelines

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.

Example

Enable destination address prefix aggregation.

```
<HUAWEI> system-view
[HUAWEI] ip netstream aggregation destination-prefix
[HUAWEI-aggregation-dstpre] enable
```

16.11.17 export version

Function

The **export version** command configures the version of exported packets carrying aggregation flow statistics.

The **undo export version** command restores the default setting.

By default, the aggregation flow statistics are exported in the version of V8.

Format

export version *version*

undo export version

Parameters

Parameter	Description	Value
version	Specifies the version number of exported packets carrying aggregation flow statistics.	The value of *version* is set to 8 or 9. The default is 8.

Views

NetStream aggregation 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 is defined in templates and is easy to combine or expand. The statistics are exported more flexibly.

V9 is supported by most NSCs for its advantages. It is recommended that you set the version of exported packets carrying aggregation flow statistics to V9.

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
```

16.11.18 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

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group 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 the IPv4 and IPv6 flow statistics collection function is enabled on the interface, statistics about unicast and multicast packets are collected.
- After the statistics collection function is enabled for IPv4 and IPv6 flows, the statistics are independent of each other.
- Currently, the flow statistics collection function can be enabled only on the main interface. If the NetStream function is enabled on the main interface but you do not set a sampling ratio using the **ip netstream sampler** command, the main interface uses the sampling ratio of 1:1000. If you set the sampling ratio, the interface uses this sampling ratio.

Example

Enable the flow statistics collection function for the incoming IPv4 packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip netstream inbound
```


16.11.19 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	-
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	-

Parameter	Description	Value
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	-
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	-

Parameter	Description	Value
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	-
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	-

Parameter	Description	Value
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 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]
```

16.11.20 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.	-
port-number	Specifies the destination UDP port number of the exported packets carrying IPv4 flow statistics.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the specified destination address belongs.	The value is the name of an existing VPN instance.

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
```

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
```

16.11.21 ip netstream export index-switch

Function

The **ip netstream export index-switch** command sets the number of digits in the interface index contained in an exported packet carrying IPv4 flow statistics.

The **undo ip netstream export index-switch** command restores the default configuration.

By default, the number of digits in interface indexes is 16.

Format

ip netstream export index-switch *index-switch*

undo ip netstream export 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 interface index supported by the NMS, the NMS cannot identify NetStream packets sent by the device.

This command is valid for V9. Before changing 16-digit interface indexes to 32-digit interface indexes, ensure that:

- The version of exported packets of original flows is V9.
- The version of exported packets carrying aggregation flow statistics is V9.

When the 32-digit interface index is used, the version of exported packets of original flows cannot be changed from V9 to V5, and the version of exported packets carrying aggregation flow statistics cannot be changed from V9 to V8.

Example

Change the number of digits in the interface index contained in an exported packet carrying IPv4 flow statistics from 16 to 32.

```
<HUAWEI> system-view
[HUAWEI] ip netstream export version 9
[HUAWEI] ip netstream export index-switch 32
```

16.11.22 ip netstream export source

Function

The **ip netstream export source** command configures the source address for the exported packets carrying IPv4 flow statistics.

The **undo ip netstream export source** command deletes the configured source address for the exported packets carrying IPv4 flow statistics.

By default, no source address is configured in the system view or aggregation view for the exported packets carrying IPv4 flow statistics.

Format

ip netstream export source *ip-address*

undo ip netstream export source

Parameters

Parameter	Description	Value
ip-address	Specifies the source IPv4 address of the exported packets carrying IPv4 flow statistics.	The parameter must be set to an existing IP address on the device.

Views

System view, NetStream aggregation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS identifies the data source according to the source IP address in NetStream packets, you need to specify the source IP address for NetStream packets.

Precautions

NetStream prefers the source IP 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.

This command must be performed; otherwise, the source address of output packets may be 0.0.0.0, and the output packets may be discarded during transmission or cannot be parsed by the NetStream server.

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
```

16.11.23 ip netstream export template timeout-rate

Function

The **ip netstream export template timeout-rate** command configures the interval at which the switch sends the NetStream export template to the NetStream server when IPv4 original or flexible flow statistics is exported in NetStream V9.

The **undo ip netstream export template timeout-rate** command restores the default setting.

By default, the switch sends the NetStream export template to the NetStream server at the interval of 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.	The value is an integer in the range from 1 to 3600, in minutes. The default value is 30.

Views

System view

Default Level

3: Management level

Usage Guidelines

When IPv4 original or flexible flow statistics is exported in NetStream V9, the NetStream server can parse the exported packets in V9 only after receiving the NetStream export template from the switch. By default, the switch sends the NetStream export template to the NetStream server at the interval of 30 minutes. You can run the **ip netstream export template timeout-rate** command to adjust the interval.

Example

Configure the switch to send the NetStream export template to the NetStream server at the interval of 10 minutes when IPv4 original or flexible flow statistics is exported in NetStream V9.

```
<HUAWEI> system-view
[HUAWEI] ip netstream export template timeout-rate 10
```

16.11.24 ip netstream export version

Function

The **ip netstream export version** command configures the version number and AS option of the exported packets carrying IPv4 flow statistics.

The **undo ip netstream export version** command restores the default setting.

By default, the version number of the exported packets carrying IPv4 original flow statistics is 5 and no AS option is used. The version number of the exported packets carrying IPv4 flexible flow statistics is 9. Packets of V9 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 or 9.

Parameter	Description	Value
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, only V9 supports 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.

The format of exported packets in V5 is fixed and is not easy to expand. The format of exported packets in V9 is defined in templates and is easy to combine or expand. The statistics are exported more flexibly.

V9 is supported by most NSCs for its advantages. It is recommended that you set the version of exported packets carrying aggregation flow statistics to V9.

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.
- To enable flexible flow statistics to be sent to the NSC to contain BGP next hop information, run the **collect ip bgp-next-hop** and **ip netstream export**

version 9 bgp-nexthop commands. Otherwise, the function does not take effect.

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
```

16.11.25 ip netstream record

Function

The **ip netstream record** command creates a 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* [**vxlan inner-ip**]

undo ip netstream record *record-name* [**vxlan inner-ip**]

Parameters

Parameter	Description	Value
record-name	Specifies the name of a flexible flow statistics template.	The value is a string of 1 to 32 case-insensitive characters without spaces or the following special characters: / \ : * ? " < > | @ ' %
vxlan inner-ip	Create a VXLAN flexible flow statistics template or enter the view of an existing VXLAN flexible flow statistics template. If this parameter is not specified, an IPv4 flexible flow statistics template is created by default or the view of an existing IPv4 flexible flow statistics template is displayed.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You need to create a flexible flow statistics template before exporting flexible flow statistics.

Precautions

Each switch supports a maximum of 16 IPv4 flexible flow statistics templates and 16 VXLAN flexible flow statistics templates. To configure a 17th 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. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can 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]
```

16.11.26 ip netstream sampler

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, an interface uses the packet-based regular sampling and the sampling ratio is 1000.

Format

ip netstream sampler fix-packets *packet-interval* { **inbound** | **outbound** }

undo ip netstream sampler [**fix-packets** *packet-interval*] { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
fix-packets *packet-interval*	Indicates the sampling ratio for packet-based regular sampling.	The value is an integer that ranges from 1 to 65535. **NOTE** For the S5731-H, S5731-S, S5731S-H, and S5731S-S, setting the sampling ratio to 1 affects the forwarding performance and can be performed on a maximum of eight interfaces. For details about how to calculate a sampling ratio, see NetStream Packet Sampling under the "NetStream Configuration" chapter in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Network Management and Monitoring*.
inbound	Samples incoming traffic on an interface.	-
outbound	Samples outgoing traffic on an interface.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group 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

You must run the **ip netstream sampler** command together with the **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 incoming IPv4 packets on GE0/0/1 to 1200.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip netstream sampler fix-packets 1200 inbound
[HUAWEI-GigabitEthernet0/0/1] ip netstream inbound
```

16.11.27 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

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
```

16.11.28 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 200 seconds.

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 300, in seconds. The default is 200.

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.

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 240 seconds.

```
<HUAWEI> system-view
[HUAWEI] ip netstream timeout active 240
```

16.11.29 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 1 to 300, in seconds. 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.

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

The inactive aging time that is configured using the **ip netstream timeout inactive** command applies to both IPv4 and IPv6 flows.

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
```

16.11.30 ipv6 netstream

Function

The **ipv6 netstream** command enables IPv6 flow statistics collection on the inbound and outbound interfaces.

The **undo ipv6 netstream** command restores the default setting.

By default, statistics collection for IPv6 flows is disabled on the inbound and outbound interfaces.

Format

ipv6 netstream { **inbound** | **outbound** }

undo ipv6 netstream { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Enables IPv6 flow statistics collection on the inbound interface.	-
outbound	Enables IPv6 flow statistics collection on the outbound interface.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To export IPv6 flow statistics, you must run the **ipv6 netstream** command to enable IPv6 flow statistics collection on the inbound interface.

Precautions

- When the IPv4 and IPv6 flow statistics collection function is enabled on the interface, statistics about unicast and multicast packets are collected.
- After the statistics collection function is enabled for IPv4 and IPv6 flows, the statistics are independent of each other.
- Currently, flow statistics collection can be enabled only on main interfaces. If statistics collection is enabled on an interface but you do not set a sampling ratio using the **ipv6 netstream sampler** command, the interface uses the sampling ratio of 1:1000. If you have set the sampling ratio, the interface uses this sampling ratio.

Example

Enable statistics collection for the incoming IPv6 flows on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ipv6 netstream inbound
```


16.11.31 ipv6 netstream export host

Function

The **ipv6 netstream export host** command configures the destination IP address and destination UDP port number for the exported packets carrying IPv6 flow statistics.

The **undo ipv6 netstream export host** command deletes the configured destination IP address and destination UDP port number for the exported packets carrying IPv6 flow statistics.

By default, no destination IP address or destination UDP port number is configured in the system view for the exported packets carrying IPv6 flow statistics.

Format

ipv6 netstream export host *ip-address port-number* [**vpn-instance** *vpn-instance-name*]

undo ipv6 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 IPv6 flow statistics.	-
port-number	Specifies the destination UDP port number of the exported packets.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the specified destination address belongs.	The value is the name of an existing VPN instance.

Views

System 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

The **netstream export ipv6 host** command configures the destination address for the exported packets carrying IPv6 original flows and flexible flows.

You can configure two destination IP addresses to implement NSC backup. To configure a third destination IP address, run the **undo ipv6 netstream export 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 IPv6 original flows to 10.1.1.1, and UDP port number to 222.

```
<HUAWEI> system-view
[HUAWEI] ipv6 netstream export host 10.1.1.1 222
```

16.11.32 ipv6 netstream export index-switch

Function

The **ipv6 netstream export index-switch** command sets the number of digits in the interface index contained in an exported packet carrying IPv6 flow statistics.

The **undo ipv6 netstream export index-switch** command restores the default setting.

By default, an interface index contains 16 digits.

Format

ipv6 netstream export index-switch *index-switch*

undo ipv6 netstream export index-switch

Parameters

Parameter	Description	Value
index-switch	Specifies the digit of the interface index.	The value is an integer that can be 16 or 32. The default is 16.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **ipv6 netstream export index-switch** command to set the number of digits in the interface index to 16 or 32.

Set the type of the interface index contained in exported packets the same as the type of the interface index that can be parsed by the NMS. For example, if the NMS can parse the 32-digit interface index, set the type of the interface index contained in exported packets to 32-digit interface index.

Prerequisites

The interface index length in exported packets can be set to 32 bits only when the NMS supports 32-bit interface index; otherwise, the NMS cannot identify the NetStream packets.

Example

Change the interface index type of the exported packets carrying IPv6 flow statistics from 16-digit to 32-digit.

```
<HUAWEI> system-view
[HUAWEI] ipv6 netstream export index-switch 32
```

16.11.33 ipv6 netstream export source

Function

The **ipv6 netstream export source** command configures the source address for the exported packets carrying IPv6 flow statistics.

The **undo ipv6 netstream export source** command deletes the configured source address for the exported packets carrying IPv6 flow statistics.

By default, no source address is configured on the device for the exported packets carrying IPv6 flow statistics.

Format

ipv6 netstream export source *ip-address*

undo ipv6 netstream export source

Parameters

Parameter	Description	Value
ip-address	Specifies the source IPv4 address of the exported packets carrying IPv6 flow statistics.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS identifies the data source according to the source IP address in NetStream packets, you need to specify the source IP address for NetStream packets.

Precautions

This command must be performed; otherwise, the source address of output packets may be 0.0.0.0, and the output packets may be discarded during transmission or cannot be parsed by the NetStream server.

Example

In the system view, set the source address for the exported packets carrying IPv6 flow statistics to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] ipv6 netstream export source 10.1.1.1
```

16.11.34 ipv6 netstream export template timeout-rate

Function

The **ipv6 netstream export template timeout-rate** command configures the interval at which the switch sends the NetStream export template to the NetStream server when IPv6 original or flexible flow statistics is exported in NetStream V9.

The **undo ipv6 netstream export template timeout-rate** command restores the default setting.

By default, the switch sends the NetStream export template to the NetStream server at the interval of 30 minutes.

Format

ipv6 netstream export template timeout-rate *timeout-interval*

undo ipv6 netstream export template timeout-rate

Parameters

Parameter	Description	Value
timeout-interval	Specifies the interval.	The value is an integer in the range from 1 to 3600, in minutes. The default value is 30.

Views

System view

Default Level

3: Management level

Usage Guidelines

When IPv6 original or flexible flow statistics is exported in NetStream V9, the NetStream server can parse the exported packets in V9 only after receiving the NetStream export template from the switch. By default, the switch sends the NetStream export template to the NetStream server at the interval of 30 minutes. You can run the **ip netstream export template timeout-rate** command to adjust the interval.

Example

Configure the switch to send the NetStream export template to the NetStream server at the interval of 10 minutes when IPv6 original or flexible flow statistics is exported in NetStream V9.

```
<HUAWEI> system-view
[HUAWEI] ipv6 netstream export template timeout-rate 10
```

16.11.35 ipv6 netstream export version

Function

The **ipv6 netstream export version** command configures the version number and AS option of the exported packets carrying IPv6 flow statistics.

The **undo ipv6 netstream export version** command restores the default setting.

By default, the version number of the exported packets carrying IPv6 flow statistics is not specified.

Format

ipv6 netstream export version *version* [**origin-as** | **peer-as**]

undo ipv6 netstream export version

Parameters

Parameter	Description	Value
version	Specifies the version of exported packets.	Only V9 is supported.
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.	-

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.

Precautions

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.

Example

Set the version of exported packets carrying IPv6 flow statistics to V9 and AS to **peer-as**.

```
<HUAWEI> system-view
[HUAWEI] ipv6 netstream export version 9 peer-as
```


16.11.36 ipv6 netstream sampler

Function

The **ipv6 netstream sampler** command configures packet sampling for IPv6 packets on an interface.

The **undo ipv6 netstream sampler** command restores the default setting.

By default, an interface uses the packet-based regular sampling and the sampling ratio is 1000.

Format

ipv6 netstream sampler fix-packets *packet-interval* { **inbound** | **outbound** }

undo ipv6 netstream sampler [**fix-packets** *packet-interval*] { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
fix-packets *packet-interval*	Indicates the sampling ratio for packet-based regular sampling.	The value is an integer that ranges from 1 to 65535. **NOTE** For the S5731-H, S5731-S, S5731S-H, and S5731S-S, setting the sampling ratio to 1 affects the forwarding performance and can be performed on a maximum of eight interfaces. For details about how to calculate a sampling ratio, see NetStream Packet Sampling under the "NetStream Configuration" chapter in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Network Management and Monitoring*.
inbound	Samples incoming traffic on an interface.	-
outbound	Samples outgoing traffic on an interface.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group 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 impact of NetStream on device performance.

Precautions

You must run the **ipv6 netstream sampler** command together with the **ipv6 netstream** command. If you run only the **ipv6 netstream sampler** command, the command does not take effect.

If you run the **ipv6 netstream sampler** command multiple times in the same view, only the latest configuration takes effect.

Example

Set the packet-based regular sampling interval for incoming IPv6 packets on GE0/0/1 to 1200.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ipv6 netstream inbound
[HUAWEI-GigabitEthernet0/0/1] ipv6 netstream sampler fix-packets 1200 inbound
```

16.11.37 mask

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**.

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
```

16.11.38 match (Flexible Flow Statistics Template View)

Function

The **match** command configures aggregation keywords for flexible flow statistics.

The **undo match** command deletes aggregation keywords configured for flexible flow statistics.

By default, no aggregation keyword for flexible flow statistics is configured in a flexible flow statistics template.

Format

match ip { **protocol** | **dscp** | **source-address** | **destination-address** | **source-port** | **destination-port** | **flow-label** | **ttl** }

match { **vlan** | **source-mac** | **destination-mac** } { **input** | **output** }

undo match ip { **protocol** | **dscp** | **source-address** | **destination-address** | **source-port** | **destination-port** | **flow-label** | **ttl** }

undo match { **vlan** | **source-mac** | **destination-mac** } { **input** | **output** }

Parameters

Parameter	Description	Value
ip	Aggregates statistics based on packet information at the network layer or transport layer.	-
protocol	Aggregates statistics based on the protocol type.	-
dscp	Aggregates statistics based on the DSCP priority.	-
source-address	Aggregates statistics based on the source IP address.	-
destination-address	Aggregates statistics based on the destination IP address.	-
source-port	Aggregates statistics based on the source port number.	-
destination-port	Aggregates statistics based on the destination port number.	-
flow-label	Aggregates statistics based on the IPv6 flow label.	-
ttl	Aggregates statistics based on the TTL value.	-
vlan	Aggregates statistics based on the VLAN ID.	-
source-mac	Aggregates statistics based on the source MAC address.	-
destination-mac	Aggregates statistics based on the destination MAC address.	-

Parameter	Description	Value
input	Aggregates statistics about incoming packets. **NOTE** If this parameter is specified, the flexible flow statistics template can be applied only to the inbound direction of an interface.	-
output	Aggregates statistics about outgoing packets. **NOTE** If this parameter is specified, the flexible flow statistics template can be applied only to the outbound direction of an interface.	-

Views

Flexible flow statistics template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

During exporting of flexible flow statistics, you can run the **match** command to configure aggregation keywords for flexible flow statistics.

Precautions

If you run this command multiple times, you can obtain a collection of multiple aggregation keywords. However, the **input** and **output** keywords cannot coexist in a flexible flow statistics template, regardless of whether the aggregation keywords before **input**/**output** are the same.

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.

Example

Set the flexible flow statistics template **abc123** to aggregate flows based on the source port number.

```
<HUAWEI> system-view
[HUAWEI] ip netstream record abc123
[HUAWEI-record-abc123] match ip source-port
```


16.11.39 port ip netstream record

Function

The **port ip netstream record** command applies a flexible flow statistics template to an interface.

The **undo port ip netstream record** command unbinds a specified flexible flow statistics template from an interface.

By default, no flexible flow statistics template is applied to an interface.

Format

port ip netstream record *record-name* [**vxlan inner-ip**] [**inbound** | **outbound**]

undo port ip netstream record [*record-name* [**vxlan inner-ip**] [**inbound** | **outbound**]]

NOTE

If neither **inbound** nor **outbound** is configured, the flexible flow statistics template is applied to both the inbound and outbound directions of an interface.

Parameters

Parameter	Description	Value
record-name	Specifies the name of a flexible flow statistics template.	The value must be the name of an existing flexible flow statistics template.
inbound	Applies the flexible flow statistics template to the inbound direction of an interface.	-
outbound	Applies the flexible flow statistics template to the outbound direction of an interface.	-
vxlan inner-ip	Applies a VXLAN flexible statistics template to an interface.	-

Views

GE interface view, XGE interface view, MultiGE interface view, 25GE interface view, 40GE interface view, 100GE interface view, port group 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

A flexible flow statistics template has been created using the **ip netstream record** command, and at least one aggregation keyword has been configured using the **match** command in the flexible flow statistics template view.

Precautions

- If the **vlan** parameter is configured in the flexible flow statistics template, it is recommended that the template be applied to Layer 2 Ethernet interfaces.
- If the **input** parameter is configured in the flexible flow statistics template, the template can be applied only to the inbound direction of an interface. If the **output** parameter is configured in the flexible flow statistics template, the template can be applied only to the outbound direction of an interface.
- The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. Run the **undo port ip netstream record** command to unbind a specified flexible flow statistics template from the interface, and then you can modify or delete the template.
- Each direction of an interface can have only one flexible flow statistics template applied. The templates applied to the inbound and outbound directions of an interface can be the same or different. To change a flexible flow statistics template, run the **undo port ip netstream record** command to delete the existing template.

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 the template to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] ip netstream record abc1
[HUAWEI-record-abc1] match ip source-address
[HUAWEI-record-abc1] match ip destination-address
[HUAWEI-record-abc1] collect counter packets
[HUAWEI-record-abc1] collect interface input
[HUAWEI-record-abc1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port ip netstream record abc1
```


16.11.40 refresh netstream template

Function

The **refresh netstream template** command immediately refreshes the NetStream export template.

By default, the template is refreshed every 30 minutes.

Format

refresh netstream template

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

After a NetStream server restarts, you need to run this command to enable the device to immediately resend the NetStream export template. Only the V9 template supports this command.

Example

Refresh the NetStream export template.

```
<HUAWEI> refresh netstream template
```

16.11.41 reset ip netstream cache

Function

The **reset ip netstream cache** command forcibly ages all the flows in the cache.

Format

reset ip netstream cache slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value depends on the actual configuration.

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.

NOTE

If you run the **reset ip netstream cache** command on the device before the inactive aging time is reached, the NDE does not export the flow statistics to the NSC.

Example

Age all the flows forcibly in slot 0.

```
<HUAWEI> system-view
[HUAWEI] reset ip netstream cache slot 0
```

16.11.42 reset ip netstream statistics

Function

The **reset ip netstream statistics** command deletes NetStream flow statistics.

Format

reset ip netstream statistics slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value depends on the actual configuration.

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 statistics** 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 in slot 0.

```
<HUAWEI> reset ip netstream statistics slot 0
```

16.11.43 template timeout-rate

Function

The **template timeout-rate** command configures the interval at which the switch sends the NetStream export template to the NetStream server when IPv4 aggregation flow statistics is exported in NetStream V9.

The **undo template timeout-rate** command restores the default setting.

By default, the switch sends the NetStream export template to the NetStream server at the interval of 30 minutes.

Format

template timeout-rate *timeout-interval*

undo template timeout-rate

Parameters

Parameter	Description	Value
timeout-interval	Specifies the interval.	The value is an integer in the range from 1 to 3600, in minutes. The default value is 30.

Views

NetStream aggregation view

Default Level

3: Management level

Usage Guidelines

When IPv4 aggregation flow statistics is exported in NetStream V9, the NetStream server can parse the exported packets in V9 only after receiving the NetStream export template from the switch. By default, the switch sends the NetStream export template to the NetStream server at the interval of 30 minutes. You can run the **ip netstream export template timeout-rate** command to adjust the interval.

Example

Configure the switch to send the NetStream export template to the NetStream server at the interval of 10 minutes when IPv4 aggregation flow statistics is exported in NetStream V9.

```
<HUAWEI> system-view
[HUAWEI] ip netstream aggregation source-prefix
[HUAWEI-aggregation-srcpre] template timeout-rate 10
```

16.12 sFlow Configuration Commands

NOTE

sFlow collects statistics and analyzes service traffic. During service provisioning, personal data may be involved. You have an obligation to make privacy policies and take measures according to the applicable law of the country to protect personal data.

16.12.1 Command Support

Only the following switch models support sFlow:

S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6720S-S, S6735-S, S6720-EI, S6720S-EI

16.12.2 display sflow

Function

The **display sflow** command displays the sFlow configuration on a specified device.

Format

display sflow [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the sFlow information on a device, where *slot-id* specifies the slot ID of the device. If this parameter is not configured, the global sFlow configuration is displayed.	The value is an integer and must be set according to the device configuration.

Views

All views

Default Level

3: Management level

Usage Guidelines

After configuring the sFlow function, you can use the **display sflow** command to verify the configuration.

The **display sflow** command shows the sFlow configuration, which helps you locate faults.

Example

Display the sFlow configuration on a specified device.

```
<HUAWEI> display sflow slot 0
sFlow Version 5 Information:
------------------------------------------------------------------------------
Agent Information:

    IP Address: 192.168.1.206(CLI)
 Address family: IPV4
   Vpn-instance: NA
------------------------------------------------------------------------------
```



```
Collector Information:

  Collector ID: 1
    IP Address: 192.168.1.194
 Address family: IPV4
  Vpn-instance: NA
          Port: 6343
 Datagram size: 1500
     Time out: NA
   Description: zjm-pc
------------------------------------------------------------------------------
Port on slot 0 Information:

Interface: GE0/0/1
  Flow-sample collector: 1          Counter-sample collector  : 1
  Flow-sample rate(1/x): 2048       Counter-sample interval(s): 10
  Flow-sample maxheader: 64
  Flow-sample direction: IN,OUT
<HUAWEI> display sflow slot 0
sFlow Version 5 Information:
------------------------------------------------------------------------------
Agent Information:

    IP Address: 192.168.1.20(Auto)
 Address family: IPV4
  Vpn-instance: NA
 Related collector: 1
------------------------------------------------------------------------------
Collector Information:

  Collector ID: 1
    IP Address: 192.168.1.94
 Address family: IPV4
  Vpn-instance: NA
          Port: 6343
 Datagram size: 1400
     Time out: NA
   Description: NA
------------------------------------------------------------------------------
Port on slot 0 Information:

Interface: GE0/0/2
 Flow-sample collector: NA         Counter-sample collector  : NA
 Flow-sample rate(1/x): 257        Counter-sample interval(s): 2
 Flow-sample maxheader: 512
 Flow-sample direction: IN
```

Table 16-79 Description of the **display sflow** command output

Item	Description
sFlow Version 5 Information	Configuration information about sFlow V5.
Agent Information	Configuration of the sFlow Agent.

Item	Description
IP Address	IP address of the sFlow Agent. To configure this parameter, run the **sflow agent** command. The string in the parentheses next to the IP address can be: ● CLI: Indicate that this IP address is specified using the **sflow agent** command. ● Auto: Indicate that the sFlow agent uses the IP address of the outbound interface in the route to the sFlow collector as the sFlow agent IP address.
Address family	Address family of the sFlow Agent: ● IPV4: IPv4 address family ● IPV6: IPv6 address family To configure this parameter, run the **sflow agent** command.
Vpn-instance	VPN instance of the sFlow Agent. To configure this parameter, run the **sflow agent** command. The value will be NA if this parameter is not configured in the **sflow agent** command.
Related collector	Collector ID corresponding to the IP address automatically selected by the sFlow agent.
Collector Information	Configuration of the sFlow Collector.
Collector ID	ID of the sFlow Collector. To configure this parameter, run the **sflow collector** command.
IP Address	IP address of the sFlow Collector. To configure this parameter, run the **sflow collector** command.
Address family	Address family of the sFlow collector: ● IPV4: IPv4 address family ● IPV6: IPv6 address family To configure this parameter, run the **sflow collector** command.
Vpn-instance	VPN instance of the sFlow Collector. To configure this parameter, run the **sflow collector** command. The value will be NA if this parameter is not configured in the **sflow collector** command.
Port	Port number of the sFlow Collector. To configure this parameter, run the **sflow collector** command.
Datagram size	Maximum length of sFlow packets sent to the sFlow Collector. To configure this parameter, run the **sflow collector** command.

Item	Description
Time out	Aging time of the sFlow Collector. To configure this parameter, run the **sflow collector** command. The value will be NA if this parameter is not configured or is set to 0 in the **sflow collector** command.
Description	Description of the sFlow Collector. To configure this parameter, run the **sflow collector** command. The value will be NA if this parameter is not configured in the **sflow collector** command.
Port on slot 0 Information	sFlow configuration on the interface in slot 0.
Interface	sFlow-enabled interface. To configure this parameter, run the **sflow flow-sampling collector** command.
Flow-sample collector	sFlow Collector that receives flow sampling data. To configure this parameter, run the **sflow flow-sampling collector** command.
Counter-sample collector	sFlow Collector that receives counter sampling data. To configure this parameter, run the **sflow counter-sampling collector** command.
Flow-sample rate(1/x)	Flow sampling rate. To configure this parameter, run the **sflow flow-sampling rate** command.
Counter-sample interval(s)	Counter sampling interval. To configure this parameter, run the **sflow counter-sampling interval** command.
Flow-sample maxheader	The maximum bytes of data that can be copied from a sampled packet in flow sampling. To configure this parameter, run the **sflow flow-sampling max-header** command.
Flow-sample direction	Flow sampling direction: • IN: Enable flow sampling in the inbound direction. • OUT: Enable flow sampling in the outbound direction. • IN,OUT: Enable flow sampling in both inbound direction and outbound direction. To configure this parameter, run the **sflow flow-sampling** command.

16.12.3 display sflow statistics

Function

The **display sflow statistics** command displays sFlow statistics.

Format

display sflow statistics [**slot** *slot-id* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a device.	The value is an integer and must be set according to the device configuration.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display sflow statistics** command displays sFlow statistics, including the sampling mode, number of sampled packets, sequence number of sent packets, and number of discarded sFlow packets because of expiration. You can use the command output to locate faults.

Example

Display sFlow statistics.

```
<HUAWEI> display sflow statistics
sFlow Version 5 statistic Information:
------------------------------------------------------------------------------
Collector 1 Current sample sequence:22388
------------------------------------------------------------------------------
Port on slot 0 statistic Information:

Interface: GE0/0/1
Flow-sample sequence    : 7         Counter-sample sequence : 44778
Flow-sample inbound pool: 28000       Flow-sample outbound pool: 4000
------------------------------------------------------------------------------
```

Table 16-80 Description of the **display sflow statistics** command output

Item	Description
sFlow Version 5 statistic Information	sFlow sampling of sFlow version 5.

Item	Description
Collector 1 Current sample sequence	Sampling sequence number of the sFlow collector.
Port on slot 0 statistic Information	sFlow sampling information on slot 0.
Interface: GE0/0/1	sFlow-enabled interface.
Flow-sample sequence	Sequence number for flow sampling on an interface.
Counter-sample sequence	Sequence number for counter sampling on an interface.
Flow-sample inbound pool	Number of incoming packets for flow sampling on an interface.
Flow-sample outbound pool	Number of outgoing packets for flow sampling on an interface.

16.12.4 sflow agent

Function

The **sflow agent** command creates an sFlow agent and specifies an IP address for the sFlow agent or updates the IP address of the existing sFlow agent.

The **undo sflow agent** command deletes the IP address of an sFlow agent.

By default, an sFlow agent uses the IP address of the outbound interface in the route to the sFlow collector as the sFlow agent IP address of sFlow packets.

Format

sflow agent { **ip** [**vpn-instance** *vpn-instance-name*] *ip-address* | **ipv6** [**vpn-instance** *vpn-instance-name*] *ipv6-address* }

undo sflow agent { **ip** [**vpn-instance** *vpn-instance-name*] *ip-address* | **ipv6** [**vpn-instance** *vpn-instance-name*] *ipv6-address* }

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies the IPv4 address of an sFlow agent.	The value is in dotted decimal notation and is a valid unicast address except 127.X.X.X.

Parameter	Description	Value
ipv6 *ipv6-address*	Specifies an IPv6 address of the sFlow agent.	The value is an IPv6 unicast address, which is a 32-digit hexadecimal number.
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.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

sFlow is a traffic monitoring technique that collects and analyzes traffic statistics. An sFlow agent encapsulates traffic statistics into sFlow packets and sends the sFlow packets to specified sFlow collectors. To send the sFlow packets to a certain sFlow collector, configure an IP address for the sFlow agent as the source address of sFlow packets. The sFlow collector analyzes and displays the traffic statistics based on the traffic in the received sFlow packets. Network administrators can view the traffic statistics on a specified interface based on the IP address of the sFlow agent and interface number.

Prerequisites

- The IP address configured as the source address must exist on the device.
- A VPN instance has been created if the sFlow agent is located on a private network.

Configuration Impact

If you run the **sflow agent** command multiple times, only the latest configuration takes effect.

Precautions

A maximum of two sFlow agents can be configured in the system, and each VPN instance of an address family supports only one agent. The IP address of an agent must be a valid unicast IP address of an interface. If an IPv6 address is specified for an agent, the IPv6 address must be a global unicast address, but cannot be a link-local address.

Example

Configure an IPv4 address for the sFlow agent.

```
<HUAWEI> system-view
[HUAWEI] sflow agent ip 192.168.100.10
```

Configure an IPv6 address for the sFlow agent.

```
<HUAWEI> system-view
[HUAWEI] sflow agent ipv6 FC00::1
```

16.12.5 sflow collector

Function

The **sflow collector** command creates an sFlow collector and sets or modifies optional parameters for the sFlow collector.

The **undo sflow collector** command restores default values of optional parameters of the sFlow collector or deletes the sFlow collector.

By default, no sFlow collector is configured.

Format

sflow collector *collector-id* { **ip** [**vpn-instance** *vpn-instance-name*] *ip-address* | **ipv6** [**vpn-instance** *vpn-instance-name*] *ipv6-address* } [**datagram-size** *datagram-size* | **port** *port-num* | **time-out** *time*] * [**description** *description*]

sflow collector *collector-id* { **datagram-size** *datagram-size* | **port** *port-num* } * [**description** *description*]

undo sflow collector *collector-id* [**datagram-size** | **port** | **description**] *

Parameters

Parameter	Description	Value
collector-id	Specifies the ID of an sFlow collector. This ID is used when you specify the collector in subsequent sFlow configuration.	The value is an integer that can be 1 or 2.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
ip-address	Specifies an IPv4 address of the sFlow collector.	The value is a value unicast IP address in X.X.X.X format, dotted decimal notation. The value cannot be 127.X.X.X.

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address for the sFlow collector.	The value is a 32-digit hexadecimal number in the format of X:X:X:X:X:X:X:X and is a valid global IPv6 unicast address.
datagram-size *datagram-size*	Specifies the maximum length of sFlow packets sent from an sFlow agent to an sFlow collector.	The value is an integer, in bytes. It ranges from 1024 to 8100. The default value is 1400.
port *port-num*	Specifies the UDP destination port number of sFlow packets.	The value is an integer that ranges from 1 to 65535. The default value is 6343.
description *description*	Specifies the description of an sFlow collector.	The value is a string of 1 to 255 case-sensitive characters without spaces.
time-out *time*	Specifies the aging time of an sFlow collector.	The value is an integer that ranges from 0 to 3600, in seconds. The default value is 0, indicating that the sFlow collector is not aged out. If the default value is used, the aging time cannot be changed.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage scenario

sFlow is a traffic monitoring technique that collects and analyzes traffic statistics. An sFlow agent encapsulates traffic statistics into sFlow packets and sends the sFlow packets to all sFlow collectors. To send the sFlow packets to a certain sFlow collector, configure an sFlow collector used to receive sFlow packets and analyze traffic of sFlow packets. When both flow sampling and counter sampling are configured on an interface of an sFlow agent, the sFlow agent sends the flow

sampling data and counter sampling data to one or two sFlow collectors. Because sFlow packets are sampled quickly and the number of sFlow packets sent every second is limited, run the **sflow collector** command with **datagram-size length** specified to set the maximum length of sFlow packets so that an sFlow packet carries more sampled data. This reduces the number of sent sFlow packets.

NOTE

When you create an sFlow collector, specify the ID and IP address for the sFlow collector. If the aging time of the sFlow collector is not set, the sFlow collector is not aged out by default and the aging time cannot be changed.

Prerequisites

- There is a reachable route between an sFlow agent and an sFlow collector.
- A VPN instance has been created if the sFlow collector is located on a private network.

Configuration Impact

If you run the **sflow collector** command multiple times on the same address family and VPN instance, only the latest configuration takes effect.

Precautions

A maximum of two sFlow collectors can be configured in the system.

Example

Configure an IPv4 address for the sFlow collector, and set the aging time of the sFlow collector to 100s.

```
<HUAWEI> system-view
[HUAWEI] sflow collector 1 ip 192.168.100.10 time-out 100
```

Configure an IPv6 address for the sFlow collector, and set the aging time of the sFlow collector to 100s.

```
<HUAWEI> system-view
[HUAWEI] sflow collector 1 ipv6 FC00::1 time-out 100
```

16.12.6 sflow counter-sampling collector

Function

The **sflow counter-sampling collector** command specifies the target sFlow collector that receives counter sampling data.

The **undo sflow counter-sampling collector** command deletes the target sFlow collector.

By default, no target sFlow collector is specified.

Format

sflow counter-sampling collector { *collector-id* | **all** }

undo sflow counter-sampling collector { *collector-id* | **all** }

Parameters

Parameter	Description	Value
collector-id	Specifies the ID of the target sFlow collector that receives counter sampling data.	The value is an integer that can be 1 or 2. **NOTE** The value of *collector-id* is set using the **sflow collector** command.
all	Indicates all the configured sFlow collectors.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage scenario

Counter sampling is based on time. An sFlow agent periodically obtains traffic statistics on an interface, encapsulates the traffic statistics into sFlow packets, and sends them to an sFlow collector. When multiple sFlow collectors are configured, you can run the **sflow counter-sampling collector** command to specify the target sFlow collector to receive the counter sampling data. Each interface can send sFlow sampling data to a maximum of two sFlow collectors.

When you run the **sflow counter-sampling collector** command to specify the first target sFlow collector on an interface, counter sampling is enabled on the interface. When you run the **undo sflow counter-sampling collector** command to delete the last target sFlow collector on an interface, counter sampling is disabled on the interface.

Prerequisites

An sFlow collector has been created using the **sflow collector** command.

Precautions

The **sflow flow-sampling rate** command only applies to Layer 2 physical interfaces, but does not apply to Eth-Trunk or Layer 3 interfaces. However, this command takes effect on the Layer 3 interface which is switched from a Layer 2 interface using the **undo portswitch** command, and can take effect on Eth-Trunk member interfaces.

Example

Specify sFlow collector 1 to receive counter sampling data.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] sflow counter-sampling collector 1
```

Configure a port group **pg1** that has member ports GE0/0/2 and GE0/0/3, and specify sFlow collector 1 to receive counter sampling data for the port group **pg1**.

```
[HUAWEI] port-group pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/2
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/3
[HUAWEI-port-group-pg1] sflow counter-sampling collector 1
```

16.12.7 sflow counter-sampling interval

Function

The **sflow counter-sampling interval** command sets the counter sampling interval on an interface.

The **undo sflow counter-sampling interval** command restores the default counter sampling interval on an interface.

By default, the counter sampling interval on an interface is 10s.

Format

sflow counter-sampling interval *interval*

undo sflow counter-sampling interval

Parameters

Parameter	Description	Value
interval *interval*	Specifies the counter sampling interval.	The value is an integer that ranges from 2 to 3600, in seconds. The default value is 10.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage scenario

Counter sampling is based on time. An sFlow agent periodically obtains traffic statistics on an interface, encapsulates the traffic statistics into sFlow packets, and sends them to an sFlow collector. You can run the **sflow counter-sampling interval** command to set an appropriate counter sampling interval.

Precautions

The **sflow flow-sampling rate** command only applies to Layer 2 physical interfaces, but does not apply to Eth-Trunk or Layer 3 interfaces. However, this command takes effect on the Layer 3 interface which is switched from a Layer 2 interface using the **undo portswitch** command, and can take effect on Eth-Trunk member interfaces. If you run the **sflow flow-sampling rate** command multiple times, only the latest configuration takes effect.

Example

Set the counter sampling interval to 100s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] sflow counter-sampling interval 100
```

Configure a port group **pg1** that has member ports GE0/0/2 and GE0/0/3, and set the counter sampling interval to 100s for the port group **pg1**.

```
[HUAWEI] port-group pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/2
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/3
[HUAWEI-port-group-pg1] sflow counter-sampling interval 100
```

16.12.8 sflow flow-sampling

Function

The **sflow flow-sampling** command enables flow sampling in a specified direction on an interface.

The **undo sflow flow-sampling** command disables flow sampling in a specified direction on an interface.

By default, flow sampling is enabled in both directions on an interface.

Format

sflow flow-sampling { **inbound** | **outbound** }

undo sflow flow-sampling { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Enables flow sampling in the inbound direction.	-
outbound	Enables flow sampling in the outbound direction.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage scenario

You can specify the direction in which flow sampling is performed. Flow sampling can be performed in both inbound and outbound directions.

Precautions

The **sflow flow-sampling rate** command only applies to Layer 2 physical interfaces, but does not apply to Eth-Trunk or Layer 3 interfaces. However, this command takes effect on the Layer 3 interface which is switched from a Layer 2 interface using the **undo portswitch** command, and can take effect on Eth-Trunk member interfaces. If you run the **sflow flow-sampling rate** command multiple times, only the latest configuration takes effect.

Example

Enable flow sampling in the inbound direction.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] sflow flow-sampling inbound
```

Configure a port group **pg1** that has member ports GE0/0/2 and GE0/0/3, and enable flow sampling in the inbound direction of the port group **pg1**.

```
[HUAWEI] port-group pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/2
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/3
[HUAWEI-port-group-pg1] sflow flow-sampling inbound
```

16.12.9 sflow flow-sampling collector

Function

The **sflow flow-sampling collector** command specifies the target sFlow collector that receives flow sampling data.

The **undo sflow flow-sampling collector** command deletes the target sFlow collector that receives flow sampling data.

By default, no target sFlow collector is specified.

Format

sflow flow-sampling collector { *collector-id* | **all** }

undo sflow flow-sampling collector { *collector-id* | **all** }

Parameters

Parameter	Description	Value
collector-id	Specifies the ID of the target sFlow collector that receives flow sampling data.	The value is an integer that can be 1 or 2.
all	Indicates all the configured sFlow collectors.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage scenario

An sFlow agent samples packets in a direction of an interface based on a sampling rate, analyzes packets, encapsulates sampled packets and analysis result into sFlow packets, and then sends the sFlow packets to an sFlow collector. When multiple sFlow collectors are configured, you can run the **sflow flow-sampling collector** command to specify one or two to receive sFlow packets. Each interface can send sFlow sampling packets to a maximum of two collectors.

When you run the **sflow flow-sampling collector** command to specify the first target sFlow collector on an interface, flow sampling is enabled on the interface. When you run the **undo sflow flow-sampling collector** command to delete the last target sFlow collector on an interface, flow sampling is disabled on the interface.

Prerequisites

An sFlow collector has been created using the **sflow collector** command.

Precautions

The **sflow flow-sampling rate** command only applies to Layer 2 physical interfaces, but does not apply to Eth-Trunk or Layer 3 interfaces. However, this command takes effect on the Layer 3 interface which is switched from a Layer 2

interface using the **undo portswitch** command, and can take effect on Eth-Trunk member interfaces.

Example

Specify sFlow collector 1 to receive the flow sampling data.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] sflow flow-sampling collector 1
```

Configure a port group **pg1** that has member ports GE0/0/2 and GE0/0/3, and specify sFlow collector 1 to receive flow sampling data for the port group **pg1**.

```
[HUAWEI] port-group pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/2
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/3
[HUAWEI-port-group-pg1] sflow flow-sampling collector 1
```

16.12.10 sflow flow-sampling max-header

Function

The **sflow flow-sampling max-header** command sets the maximum bytes of data that can be copied from a sampled packet in flow sampling.

The **undo sflow flow-sampling max-header** command restores the default maximum bytes of data.

By default, a maximum of 64 bytes of data can be copied from a sampled packet in flow sampling.

Format

sflow flow-sampling max-header *length*

undo sflow flow-sampling max-header

Parameters

Parameter	Description	Value
length	Specifies the maximum bytes of data that can be copied from a sampled packet.	The unit is byte. The value is an integer that ranges from 18 to 512. The default value is 64.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage scenario

An sFlow agent samples packets in a direction of an interface based on a sampling rate, analyzes packets, encapsulates sampled packets and analysis result into sFlow packets, and then sends the sFlow packets to an sFlow collector. The datagram size of sFlow packets is set using the **sflow collector** [**datagram-size** *datagram-size*] command. If only the information carried in the packet header is required, run the **sflow flow-sampling max-header** command to set the maximum length of data starting from the original packet header that can be copied from a sampled packet.

Precautions

The **sflow flow-sampling rate** command only applies to Layer 2 physical interfaces, but does not apply to Eth-Trunk or Layer 3 interfaces. However, this command takes effect on the Layer 3 interface which is switched from a Layer 2 interface using the **undo portswitch** command, and can take effect on Eth-Trunk member interfaces.

Example

Set the maximum length of data starting from the original packet header that can be copied from a sampled packet to 256 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] sflow flow-sampling max-header 256
```

Configure a port group **pg1** that has member ports GE0/0/2 and GE0/0/3, and set the maximum length of data starting from the original packet header that can be copied from a sampled packet to 256 bytes for the port group **pg1**.

```
[HUAWEI] port-group pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/2
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/3
[HUAWEI-port-group-pg1] sflow flow-sampling max-header 256
```

16.12.11 sflow flow-sampling rate

Function

The **sflow flow-sampling rate** command sets the sampling rate on an interface.

The **undo sflow flow-sampling rate** command restores the default sampling rate on an interface.

By default, the sampling rate on a 40GE interface is 1/20480 and on other types of interfaces is 1/2048.

Format

sflow flow-sampling rate *rate*

undo sflow flow-sampling rate

Parameters

Parameter	Description	Value
rate *rate*	Specifies the sampling rate in the format of 1/*rate*. *rate* specifies the number of packets out of which the interface will sample a packet.	The *rate* is an integer that ranges from 256 to 65535 on the S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735-S-I, and S5735S-S, and ranges from 256 to 1048576 on other devices.

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, MultiGE interface view, 40GE interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage scenario

An sFlow agent samples packets in a direction of an interface based on a sampling rate, analyzes packets, encapsulates sampled packets and analysis result into sFlow packets, and then sends the sFlow packets to an sFlow collector. You can run the **sflow flow-sampling rate** command to set the sampling rate to limit the number of sampled packets.

Precautions

The **sflow flow-sampling rate** command only applies to Layer 2 physical interfaces, but does not apply to Eth-Trunk or Layer 3 interfaces. However, this command takes effect on the Layer 3 interface which is switched from a Layer 2 interface using the **undo portswitch** command, and can take effect on Eth-Trunk member interfaces. If you run the **sflow flow-sampling rate** command multiple times, only the latest configuration takes effect.

Example

Set the sampling rate to 1/3072.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] sflow flow-sampling rate 3072
```

Configure a port group **pg1** that has member ports of GE0/0/2 and GE0/0/3, and set the sampling rate to 1/3072 for the port group **pg1**.

```
[HUAWEI] port-group pg1
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/2
```



```
[HUAWEI-port-group-pg1] group-member gigabitethernet 0/0/3
[HUAWEI-port-group-pg1] sflow flow-sampling rate 3072
```

16.13 Ping and Tracert Configuration Commands

16.13.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.13.2 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** | { **-f** | **ignore-mtu** } | **-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*] * *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.

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*, that is, performing a Ping test with multiple Ping packets. 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.

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 Response packets. This process prevents ping failures caused by incorrect routing entries. **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.	The value is in dotted decimal notation.
-i *interface-type interface-number*	Specifies the outbound interface for sending ICMP Echo Request packets. **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.	-

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.

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, that is, performing a Ping test with large-sized Ping packets.	The value is an integer that ranges from 20 to 9600, in bytes. The default value is 56.

Parameter	Description	Value
-range	Enables the device to send ICMP Echo Request messages with variable payload lengths. **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.	• 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.
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.

Parameter	Description	Value
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.	-
-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 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. The minimum timeout period is 200 ms. If the specified timeout period is less than 200 ms, the device uses 200 ms as the timeout period.
-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	• 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.	-

Parameter	Description	Value
-vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.
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:

- Scenario 1: 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.

- Scenario 2: 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.
- Scenario 3: 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.
- Scenario 4: 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.
- Scenario 5: Check the path MTU. You can run the **ping -f -s** *packetsize host* command to prevent ICMP message fragmentation and set the length of an ICMP message so as to obtain the path MTU through multiple probes.
- Scenario 6: 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.

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

- 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.
- To ensure security, 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.
- The **ping** command is typically used to check network connectivity and link quality, and cannot be used to evaluate the forwarding latency of a switch. If the pinged IP address is not the local switch's, the switch forwards the ICMP packet according to routing entries, without sending them to the CPU. If the pinged IP address is the local switch's, the switch sends the ICMP packets to the CPU for processing. In this case, you can run the **icmp-reply fast** command on the switch to enable the fast ICMP reply function. With this function, the switch directly processes the ICMP packets destined for its own IP address on interfaces, without sending the packets to the CPU. This minimizes the ping latency.
- When the ping command is used, packet statistics are collected only in the outbound direction of interfaces on the S1720GW-E, S1720GWR-E, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S6720S-S.

Example

Check whether the host at 10.1.1.2 is reachable.

```
<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 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
```

Enable the device to send ICMP Echo Request messages with variable payload lengths.

```
<HUAWEI> ping -range min 56 max 60 192.168.1.9
  PING 192.168.1.9: 56-60  data bytes, press CTRL_C to break
    Reply from 192.168.1.9: bytes=56 Sequence=1 ttl=255 time=80 ms
    Reply from 192.168.1.9: bytes=57 Sequence=2 ttl=255 time=60 ms
    Reply from 192.168.1.9: bytes=58 Sequence=3 ttl=255 time=80 ms
    Reply from 192.168.1.9: bytes=59 Sequence=4 ttl=255 time=80 ms
    Reply from 192.168.1.9: bytes=60 Sequence=5 ttl=255 time=50 ms

  --- 192.168.1.9 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 50/70/80 ms
```

Check whether the host at 10.1.1.10 is reachable.

```
<HUAWEI> ping 10.1.1.10
ping 10.1.1.10
  PING 10.1.1.10: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.10: bytes=56 Sequence=1 ttl=128 time=1 ms
    Reply from 10.1.1.10: bytes=56 Sequence=1 ttl=64 time=1 ms (DUP!)
    Reply from 10.1.1.10: bytes=56 Sequence=2 ttl=128 time=1
ms
    Reply from 10.1.1.10: bytes=56 Sequence=2 ttl=64 time=1 ms
(DUP!)
    Reply from 10.1.1.10: bytes=56 Sequence=3 ttl=128 time=1 ms
    Reply from 10.1.1.10: bytes=56 Sequence=3 ttl=64 time=1 ms (DUP!)
    Reply from 10.1.1.10: bytes=56 Sequence=4 ttl=128 time=1
ms
    Reply from 10.1.1.10: bytes=56 Sequence=4 ttl=64 time=1 ms
```



```
(DUP!)
   Reply from 10.1.1.10: bytes=56 Sequence=5 ttl=128 time=1
ms

 --- 10.1.1.10 ping statistics ---
   5 packet(s) transmitted
   9 packet(s) received
   4 duplicates
   -- somebody's printing up packets
   round-trip min/avg/max = 1/0/1 ms
```

Table 16-81 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**.
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". **NOTE** If a received packet ends with (DUP!), the device has received the Echo Reply messages with repeated sequence number.

Item	Description
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. • duplicates: indicates that the device has received the Echo Reply messages with repeated sequence number. • % packet loss: indicates the percentage of unresponded messages to total sent messages. • -- somebody's printing up packets: indicates that the number of received Echo Reply messages is larger than the number of send Echo Request 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.)

16.13.3 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*]

Parameters

Parameter	Description	Value
-a *source-ipv6-address*	Specifies a source IPv6 address for sending ICMPv6 Echo Request messages. 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 switch 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.

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 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. The minimum timeout period is 200 ms. If the specified timeout period is less than 200 ms, the device uses 200 ms as the timeout period.
-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 must be an existing VPN instance name.

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 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 16-82 Description of the ping ipv6 command output

Item	Description
PING HH:HH::HH:H	IPv6 address of the destination host.

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.

16.13.4 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* | **-v** | **-vpn-instance** *vpn-instance-name* [**pipe**] | **-w** *timeout* | **-s** *packetsize*] * *host*

NOTE

Only the S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support **-v**.

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 of 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.

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.	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 must be an existing VPN instance name.
pipe	Specifies the pipe mode. When a probe packet passes through the MPLS domain, the entire MPLS domain is considered as one hop and the IP TTL of the probe packet is reduced by one on the ingress node and egress node respectively.	-
-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 UDP payload of packets to be sent in the **tracert** command.	The value is an integer that ranges from 12 to 9600, in bytes. The default value is 12.

Parameter	Description	Value
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.

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.
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 an IPv4 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

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.

By default, each hop sends three probe packets. If load balancing is implemented, the same hop may correspond to different nodes. In this case, if the IP address in a

probe packet is different from that in the previous probe packet, information in the later probe packet is displayed. If the IP address in a probe packet is the same as that in the previous probe packet, information in the previous probe packet is displayed.

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
```

Table 16-83 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.
1 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. Tracert is used to test connectivity. When a switch is a hop in a tracert test, tracert packets are be sent to the CPU for processing. This causes a time difference, but it does not mean the link delay.

Item	Description
* * *	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.

16.13.5 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 [**-f** *first-hop-limit* | **-m** *max-hop-limit* | **-p** *port-number* | **-q** *probes* | **-w** *timeout* | **vpn-instance** *vpn-instance-name* | **-a** *source-ipv6-address* | **-s** *packetsize* | **-name** | **-v**] * *host*

NOTE

Only the S5731-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S5731S-H, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730S-H, and S6730-H support **-v**.

Parameters

Parameter	Description	Value
-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.

Parameter	Description	Value
-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.
-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 must be an existing VPN instance name.
-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.

Parameter	Description	Value
-s *packetsize*	Specifies the size of IPv6 probe packets in the **tracert ipv6** command.	The value is an integer that ranges from 20 to 9600, in bytes. The default value is 56.
-name	Displays the name of the destination host.	-
-v	Displays the MPLS label carried in the ICMP Time Exceeded packet.	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.
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

- 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
```

Table 16-84 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 30 ms 29 ms	RTT, in milliseconds.

16.14 TWAMP Light Configuration Commands

16.14.1 Command Support

Only the following switch models support TWAMP Light, and only TWAMP Light Responder function is supported:

S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S

16.14.2 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 Responder.

Format

display twamp-light responder test-session [**verbose** | *session-id*]

Parameters

Parameter	Description	Value
verbose	Displays details about all measurement sessions on the TWAMP Light Responder.	-
session-id	Displays details about the specified measurement session on the TWAMP Light Responder.	The value is an integer that ranges from 1 to 5.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the performance measurement function is enabled, you can run this command to view measurement session information on the TWAMP Light Responder 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  : 2
------------------------------------------------------------------------------
  ID    Local-IP       Local-Port    Remote-IP      Remote-Port
------------------------------------------------------------------------------
   1    10.1.1.2          10000      10.2.2.2          20000
   2    10.1.1.3          10001      10.2.2.3          20001
```

Display details about all measurement sessions.

```
<HUAWEI> display twamp-light responder test-session verbose
Session ID                    : 1
Local IP                      : 10.1.1.2
Local Port                    : 10000
Remote IP                     : 10.2.2.2
```



```
Remote Port                  : 20000
Mode                         : unauthenticated
VPN Instance                 : test
Description                  : -

Session ID                   : 2
Local IP                     : 10.1.1.3
Local Port                   : 10001
Remote IP                    : 10.2.2.3
Remote Port                  : 20001
Mode                         : unauthenticated
VPN Instance                 : shuai
Description                  : -
```

Display details about the specified measurement session.

```
<HUAWEI> display twamp-light responder test-session 1
Session ID                   : 1
Local IP                     : 10.1.1.2
Local Port                   : 10000
Remote IP                    : 10.2.2.2
Remote Port                  : 20000
Mode                         : unauthenticated
VPN Instance                 : test
Description                  : -
```

Table 16-85 Description of the **display twamp-light responder test-session** command output

Item	Description
Total number	Total number of sessions.
ID/Session ID	Session ID.
Local-IP/Local IP	IP address of the session Responder.
Local-Port/Local Port	UDP port number of the session Responder.
Remote-IP/Remote IP	IP address of the session Sender.
Remote-Port/Remote Port	UDP port number of the session Sender.
Mode	Authentication mode. The value **unauthenticated** indicates that authentication is disabled.
VPN Instance	VPN instance name. If the VPN instance name is not specified, the value of this field is empty.
Description	Session description.

16.14.3 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 configured.

Format

nqa twamp-light

undo nqa twamp-light

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Using a simple structure of TWAMP, TWAMP Light lowers the requirements on the Responder. TWAMP Light measures bidirectional network performance between any nodes on the network. 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 TWAMP Light roles, sessions, and measurement services.

Example

Create the TWAMP Light service.

```
<HUAWEI> system-view
[HUAWEI] nqa twamp-light
[HUAWEI-twamp-light]
```


16.14.4 responder

Function

The **responder** command enables the TWAMP Light Responder function and displays the TWAMP-Light-Responder view. If the Responder function has been enabled, the TWAMP-Light-Responder view is directly displayed.

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 TWAMP-Light-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]
```


16.14.5 test-session (TWAMP-Light-Responder view)

Function

The **test-session** command creates a TWAMP Light measurement session on the Responder.

The **undo test-session** command deletes a TWAMP Light measurement session on the Responder.

By default, no TWAMP Light measurement session is created on the Responder.

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*]]

Parameters

Parameter	Description	Value
session-id	Specifies the ID of the measurement session.	The value is an integer that ranges from 1 to 5.
local-ip *local-ip-address*	Specifies the IP address of the Responder.	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 Responder.	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 must be the name of an existing VPN instance.
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

After the TWAMP Light service is created, you need to create a TWAMP Light measurement session on the Responder and configure measurement instance information, including the Sender's IP address, Responder's IP address, Sender's UDP port number, Responder's UDP port number, and VPN instance name.

Precautions

- A maximum of 5 measurement sessions can be created on a Responder.
- The created session starts measurement only when the measurement starts on the Controller.
- After a session is created, its parameters cannot be modified. To modify a session, delete it and create it again.
- The IP address must be a unicast address. By default, the DSCP field in a sent packet is 0 and the packet padding length is 128.
- The UDP port of the sender must be a port that is not occupied.
- The VPN instance must exist. When the VPN instance is deleted, the related measurement instance is also deleted.

Example

Create a TWAMP Light measurement session on the Responder.

```
<HUAWEI> system-view
[HUAWEI] nqa twamp-light
[HUAWEI-twamp-light] responder
[HUAWEI-twamp-light-responder] test-session 1 local-ip 192.168.10.1 remote-ip 192.168.10.2 local-port 3000 remote-port 3001
```

16.15 NETCONF Configuration Commands

16.15.1 Command Support

NETCONF Mode	Product Model
NETCONF over SSH Callhome	S200, S5720I-SI, S5720-LI, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5720S-LI, S500, S5735-S, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731S-H, S5732-H, S5731-S, S5731S-S, S6730-S, S6730S-S, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H

NETCONF Mode	Product Model
NETCONF over SSH	All models except S1720GW-E, S1720GWR-E, and S1720X-E

16.15.2 ap manage-mode force-tradition

Function

The **ap manage-mode force-tradition** command sets the AP management mode to the local AC mode.

The **undo ap manage-mode force-tradition** command sets the AP management mode to the same as that on the switch. That is, if the NETCONF mode is enabled on the switch, the AP is managed by iMaster NCE-Campus; if the NETCONF mode is disabled on the switch, the AP is locally managed by the switch.

By default, the AP management mode is the same as that on the switch.

Format

ap manage-mode force-tradition

undo ap manage-mode force-tradition

Parameters

None

Views

NETCONF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After NETCONF is enabled on a switch (with the native AC function enabled), Fit APs are managed by iMaster NCE-Campus by default. AP entries delivered by iMaster NCE-Campus take effect, and cloud management license resources are consumed. Additionally, the switch no longer supports the commands listed in **Table 16-86**. To locally manage APs (using local AP entries and local license resources), run the **ap manage-mode force-tradition** command to set the AP management mode to the local AC mode. Then, the commands become available on the switch.

Precautions

When a Fit AP is managed by iMaster NCE-Campus, running the **ap manage-mode force-tradition** command on the switch will disconnect the Fit AP from iMaster NCE-Campus. In this case, deleting the entry of this AP on iMaster NCE-Campus will delete the corresponding AP entry on the switch synchronously. To enable the AP to go online on the switch, you need to manually confirm the AP by running the **ap-confirm** { **all** | **mac** *ap-mac* | **sn** *ap-sn* } command on the switch.

Table 16-86 Commands that are not supported by the switch in NETCONF mode

Command	Function Description
ap auth-mode { **mac-auth** | **no-auth** | **sn-auth** } **undo ap auth-mode**	Configures the AP authentication mode. For a switch in NETCONF mode, the AP authentication mode is SN authentication.
ap blacklist mac *ap-mac1* [**to** *ap-mac2*] **undo ap blacklist** { **mac** *ap-mac1* [**to** *ap-mac2*] | **all** }	Adds APs to an AP blacklist, or deletes APs from an AP blacklist.
ap modify *ap-id* **mac** *ap-mac*	Modifies the MAC address of an AP.
ap whitelist { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] } **undo ap whitelist** { **mac** { *ap-mac1* [**to** *ap-mac2*] | **all** } | **sn** { *ap-sn1* [**to** *ap-sn2*] | **all** } }	Adds APs to an AP whitelist, or deletes APs from an AP whitelist.
ap-confirm { **all** | **mac** *ap-mac* | **sn** *ap-sn* }	Confirms unauthorized APs and allows them to go online.
ap-name *ap-name*	Configures an AP name.
ap-rename { **ap-name** *name* | **ap-mac** *ap-mac-address* | **ap-id** *ap-id* } **new-name** *ap-new-name*	Changes the name of an AP.

Example

Set the AP management mode to the local AC mode.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] ap manage-mode force-tradition
```

16.15.3 assign arp netconf number

Function

The **assign arp netconf number** command sets the number of ARP entries reserved for NETCONF.

The **undo assign arp netconf number** command restores the default setting.

By default, no ARP entry is reserved for NETCONF.

Format

assign arp netconf number *number-value*

undo assign arp netconf number

Parameters

Parameter	Description	Value
number-value	Specifies the number of ARP entries reserved for NETCONF.	The value is an integer in the range from 0 to 2000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If ARP entries are used up by due to forged packet attacks, the switch cannot communicate with the NMS. To prevent this situation, you can set the number of ARP entries reserved for NETCONF communication between the switch and NMS. When the number of remaining ARP entries on a device is less than or equal to the number of ARP entries reserved for NETCONF, only ARP entries in the NETCONF scenario can be delivered.

Precautions

- When you run the **management-vlan** command in the NETCONF view to configure a management VLAN of a switch, the switch automatically delivers the **assign arp netconf number** command to set the number of ARP entries reserved for NETCONF to 200. If you then run the **undo management-vlan** command, the switch automatically delivers the **undo assign arp netconf number** command to restore the default setting.
- When you run the **source ip** command in the NETCONF view to configure a VLANIF interface for the switch to communicate with the NMS, the switch automatically delivers the **assign arp netconf number** command to set the number of ARP entries reserved for NETCONF to 200. If you then run the **undo source ip** command, the switch automatically delivers the **undo assign arp netconf number** command to restore the default setting.
- After you run this command to manually configure the number of ARP entries reserved for NETCONF and then run the **management-vlan** or **source ip** command, the system will not automatically deliver the configuration of the

number of reserved ARP entries. If you run this command to set the number of ARP entries reserved for NETCONF to 200 and then run the **undo management-vlan** or **undo source ip** command, the switch automatically delivers the **undo assign arp netconf number** command to restore the default setting; if you run this command to set the number of ARP entries reserved for NETCONF to another value and then run the **undo management-vlan** or **undo source ip** command, the system will not deliver the **undo assign arp netconf number** command to restore the default setting.

Example

Set the number of ARP entries reserved for NETCONF to 1000.

```
<HUAWEI> system-view
[HUAWEI] assign arp netconf number 1000
```

16.15.4 backup ip address (callhome template view)

Function

The **backup ip address** command configures the IPv4 address and port number of a standby NMS that communicates with a switch through NETCONF.

The **undo backup ip** command deletes the IPv4 address and port number of a standby NMS that communicates with a switch through NETCONF.

By default, no standby NMS's IPv4 address and port number are configured for communicating with a switch through NETCONF.

Format

backup ip address *ip-address* **port** *port-number*

undo backup ip address

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of the standby NMS.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of the standby NMS.	The value is an integer in the range from 1 to 65535.

Views

Callhome template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a disaster recovery scenario, you can run the **backup ip address** command to configure the IPv4 address and port number of the standby NMS that communicates with a switch through NETCONF. If the active NMS breaks down or is disconnected, services can be automatically switched to the standby NMS, ensuring service continuity.

Precautions

Assume that a switch has registered with one copy of iMaster NCE-Campus and gone online. If the switch needs to register with another copy of iMaster NCE-Campus, clear the switch configuration, run the **reset netconf db-configuration** command to clear database information from the switch, and restart the switch as prompted.

Example

Set the IP address and port number of the standby NMS that communicates with the switch through NETCONF to 10.1.2.1 and 830, respectively.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] callhome Test123
[HUAWEI-netconf-callhome-Test123] backup ip address 10.1.2.1 port 830
```

16.15.5 bootstrap

Function

The **bootstrap** command configures information about the primary Bootstrap server.

The **undo bootstrap** command deletes information about the primary Bootstrap server.

Format

bootstrap { **ip-address** *ip-address* | **domain** *domain* } **port** *port-number* **voucher-type** { **esn** | **ip-or-domain** } **always-trust**

undo bootstrap

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the Bootstrap server IP address, which is the southbound IP address of iMaster NCE-Campus.	The value is in dotted decimal notation.

Parameter	Description	Value
domain *domain*	Specifies the Bootstrap server domain name, which is the southbound domain name of iMaster NCE-Campus.	The value is a string of 3 to 128 characters.
port *port-number*	Specifies the port number of a Bootstrap server.	The value is an integer in the range from 1 to 65535. Currently, the value is fixed at 30217.
voucher-type esn	Specifies that the voucher type is the device ESN.	-
voucher-type ip-or-domain	Specifies that the voucher type is the Bootstrap server address.	-
always-trust	Specifies that the voucher returned by the Bootstrap server is trusted by default.	-

Views

NETCONF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a switch registers with the iMaster NCE-Campus, the switch needs to obtain Lite CA information from a Bootstrap server to authenticate iMaster NCE-Campus. In this scenario, you need to run the **bootstrap** command to configure information about the Bootstrap server.

Example

Configure Bootstrap server information. Assume that the southbound IP address of iMaster NCE-Campus is 1.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] bootstrap ip-address 1.1.1.1 port 30217 voucher-type ip-or-domain always-trust
```


16.15.6 backup bootstrap

Function

The **backup bootstrap** command configures information about the backup Bootstrap server.

The **undo backup bootstrap** command deletes information about the backup Bootstrap server.

Format

backup bootstrap { **ip-address** *ip-address* | **domain** *domain* } **port** *port-number* **voucher-type** { **esn** | **ip-or-domain** } **always-trust**

undo backup bootstrap

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the Bootstrap server IP address, which is the secondary southbound IP address of iMaster NCE-Campus.	The value is in dotted decimal notation.
domain *domain*	Specifies the Bootstrap server domain name, which is the secondary southbound domain name of iMaster NCE-Campus.	The value is a string of 3 to 128 characters.
port *port-number*	Specifies the port number of a Bootstrap server.	The value is an integer in the range from 1 to 65535. Currently, the value is fixed at 30217.
voucher-type esn	Specifies that the voucher type is the device ESN.	-
voucher-type ip-or-domain	Specifies that the voucher type is the Bootstrap server address.	-
always-trust	Specifies that the voucher returned by the Bootstrap server is trusted by default.	-

Views

NETCONF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a disaster recovery scenario, you can run the **backup bootstrap** command to configure information about the standby Bootstrap server. If the primary Bootstrap server breaks down or is disconnected, services are automatically switched to the backup Bootstrap server, ensuring service continuity.

Example

Configure standby Bootstrap server information. Assume that the secondary southbound IP address of iMaster NCE-Campus is 1.1.2.1.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] backup bootstrap ip-address 1.1.2.1 port 30217 voucher-type ip-or-domain always-trust
```

16.15.7 callhome

Function

The **callhome** command creates a callhome template and enters the callhome template view.

The **undo callhome** command deletes a callhome template.

By default, there is no callhome template on a switch.

Format

callhome *callhome-name*

undo callhome *callhome-name*

Parameters

Parameter	Description	Value
callhome-name	Specifies the name of a callhome template.	The value is a string of 1 to 31 case-sensitive characters excluding spaces. If the string is enclosed in double quotation marks ("), the string can contain spaces.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If iMaster NCE-Campus needs to configure and manage a switch in NETCONF over SSH Callhome mode, you must run the **callhome** command to create a callhome template so that the switch can proactively set up a NETCONF connection with iMaster NCE-Campus.

Follow-up Procedure

Run the **ip address** command in the callhome template view to configure the IPv4 address and port number for the NMS.

Precautions

Only one callhome template can be created on a switch. Before creating a new callhome template, delete the existing one by running the **undo callhome** *callhome-name* command. After the command is run, communication between the switch and NMS is interrupted.

Example

Create the callhome template **Test123** and display the callhome template view.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] callhome Test123
[HUAWEI-netconf-callhome-Test123]
```

16.15.8 card register-permit

Function

The **card register-permit** command configures a slot-to-card name mapping.

The **undo card register-permit** command disables the slot-to-card name mapping.

By default, the name of the card that can be installed in a specific slot is not specified. That is, any card can be installed in the slot.

Format

card register-permit card-id *card-id* **card-name** *card-name*

undo card register-permit card-id *card-id*

Parameters

Parameter	Description	Value
card-id *card-id*	Specifies the slot ID of a card.	The value is in the format of *Slot ID*/CARD+*Card slot ID* and is case-insensitive, for example, 1/CARD1. The slot ID is in the range 0 to 8 and the card slot ID is in the range 1 to 4.
card-name *card-name*	Specifies the name of a card.	The value is a string of 1 to 32 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In NETCONF over SSH Callhome mode, you need to specify the name of the card that can be installed in a specific slot on iMaster NCE-Campus before registering the switch with iMaster NCE-Campus. The switch can register with iMaster NCE-Campus successfully only when the required cards are installed in their corresponding slots. If the name of the card installed in a specific slot is inconsistent with that configured on iMaster NCE-Campus, the switch will set this card to the **PowerOff** state.

In NETCONF over SSH mode, after enabling the NETCONF function on the switch, run the **card register-permit** command to specify the name of the card that can be installed in a specific slot. If the name of the card installed in a specific slot is inconsistent with the configured one, the switch will set this card to the **PowerOff** state. When the NETCONF function is disabled, the slot-to-card name mappings will be automatically cleared.

Example

Specify the name of the card that can be installed on card slot 1 of the switch in slot 1 after the NETCONF function is enabled on the switch.

```
<HUAWEI> system-view
[HUAWEI] card register-permit card-id 1/card1 card-name ES5D21Q02Q00
```


16.15.9 certificate identity

Function

The **certificate identity** command configures a unique common name (CN) for the iMaster NCE-Campus's certificate, which will be used for certificate uniqueness verification.

The **undo certificate identity** command cancels the CN configuration for the iMaster NCE-Campus's certificate.

By default, no CN is configured for the iMaster NCE-Campus's certificate; that is, the switch does not verify the CN of the iMaster NCE-Campus's certificate.

Format

certificate identity *common-name*

undo certificate identity

Parameters

Parameter	Description	Value
common-name	Specifies a unique CN for the iMaster NCE-Campus's certificate.	The value can be either of the following: • A string of 1 to 64 case-insensitive characters in cleartext, with spaces not supported • A string of 48 to 108 characters in ciphertext

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

When a switch registers with iMaster NCE-Campus for authentication, bidirectional certificate authentication is performed over an SSH channel established between them to ensure secure data transmission. However, if an attacker obtains the iMaster NCE-Campus's certificate and pretends to be iMaster NCE-Campus to communicate with the switch, the switch cannot identify this forged iMaster NCE-Campus, posing security risks.

To address this issue, you can run the **certificate identity** command on the switch to specify the CN of the iMaster NCE-Campus's certificate for certificate uniqueness verification. When the switch registers with iMaster NCE-Campus

again, it compares the CN in the iMaster NCE-Campus's certificate with the locally configured one, and goes online only when the CNs are the same.

Example

Configure a CN for the iMaster NCE-Campus's certificate on the switch.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] certificate identity device-naas.huawei.com
```

16.15.10 controller backup ip-address

Function

The **controller backup ip-address** command configures an IP address of the standby iMaster NCE-Campus.

The **undo controller backup ip-address** command deletes the IP address of the standby iMaster NCE-Campus.

By default, no IP address of the standby iMaster NCE-Campus is configured.

Format

controller backup ip-address *ip-address* **port** *port-number*

undo controller backup ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the standby iMaster NCE-Campus.	The value is in dotted decimal notation.
port *port-number*	Specifies a port number.	The value is an integer in the range from 1 to 65535.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The switch needs to register with iMaster NCE-Campus for authentication in NETCONF over SSH Callhome mode. Before registration authentication, the switch

needs to obtain the IP address of iMaster NCE-Campus for communication with iMaster NCE-Campus. The switch can obtain the IP address of iMaster NCE-Campus through DHCP or the registration query center, or you can configure an IP address for iMaster NCE-Campus using the **controller ip-address** command.

In a disaster recovery scenario, you can run the **controller backup ip-address** command to configure the IP address of the standby iMaster NCE-Campus. When the active iMaster NCE-Campus breaks down or is disconnected, services are automatically switched to the standby iMaster NCE-Campus, ensuring service continuity.

Precautions

- If the switch obtains the IP addresses of iMaster NCE-Campus using all the three methods, the IP addresses are sorted in descending order of priority as follows: IP address obtained using DHCP, IP address configured using the command, and IP address obtained through the registration query center.
- If you run this command multiple times, only the latest configuration takes effect.
- When both the **controller ip-address** command and the **controller url** command are configured on the switch, only the latest command takes effect. That is, the switch registers with iMaster NCE-Campus using either the IP address of iMaster NCE-Campus or the IP address resolved from the URL of iMaster NCE-Campus.
- If a switch that has registered with a iMaster NCE-Campus registers with another iMaster NCE-Campus, the device configurations will change. Exercise caution when performing this operation.
- The configuration of this command is saved in the flash memory and therefore cannot be cleared by running the **reset netconf db-configuration** command. To clear the configuration of this command, run the **undo controller backup ip-address**, **undo netconf**, or **reset factory-configuration** command.

Example

Configure the IP address of the standby iMaster NCE-Campus on a switch.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] controller backup ip-address 10.1.1.1 port 10020
```

16.15.11 controller ip-address

Function

The **controller ip-address** command configures an IP address for iMaster NCE-Campus.

The **undo controller ip-address** command deletes the IP address configured for iMaster NCE-Campus.

By default, no IP address is configured for iMaster NCE-Campus on a switch.

Format

controller ip-address *ip-address* **port** *port-number*

undo controller ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for iMaster NCE-Campus.	The value is in dotted decimal notation.
port *port-number*	Specifies a port number.	The value is an integer in the range 1 to 65535.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The switch needs to register with iMaster NCE-Campus for authentication in NETCONF over SSH Callhome mode. Before registration authentication, the switch needs to obtain the IP address of iMaster NCE-Campus for communication with iMaster NCE-Campus. The switch can obtain the IP address of iMaster NCE-Campus through DHCP or the registration query center, or you can configure an IP address for iMaster NCE-Campus using the **controller ip-address** command.

Precautions

- If the switch obtains the IP addresses of iMaster NCE-Campus using all the three methods, the IP addresses are sorted in descending order of priority as follows: IP address obtained using DHCP, IP address configured using the command, and IP address obtained through the registration query center.
- If you run this command multiple times, only the latest configuration takes effect.
- When both the **controller ip-address** command and the **controller url** command are configured on the switch, only the latest command takes effect. That is, the switch registers with iMaster NCE-Campus using either the IP address of iMaster NCE-Campus or the IP address resolved from the URL of iMaster NCE-Campus.
- If a switch that has registered with a iMaster NCE-Campus registers with another iMaster NCE-Campus, the device configurations will change. Exercise caution when performing this operation.

- The configuration of this command is saved in the flash memory and therefore cannot be cleared by running the **reset netconf db-configuration** command. To clear the configuration of this command, run the **undo controller ip-address**, **undo netconf**, or **reset factory-configuration** command.

Example

Configure an IP address for iMaster NCE-Campus.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] controller ip-address 10.1.1.1 port 10020
```

16.15.12 controller url

Function

The **controller url** command configures a URL for iMaster NCE-Campus.

The **undo controller url** deletes the URL configured for iMaster NCE-Campus.

By default, no URL is configured for iMaster NCE-Campus on the switch.

Format

controller url *url-string* **port** *port-number*

undo controller url

Parameters

Parameter	Description	Value
url-string	Specifies a URL for iMaster NCE-Campus.	The value is a string of 3 to 128 case-sensitive characters. If you need to set one or more consecutive spaces, enclose the URL in double quotation marks (").
port *port-number*	Specifies a port number.	The value is an integer in the range 1 to 65535.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In NETCONF over SSH Callhome mode, the switch needs to register with iMaster NCE-Campus for authentication. Before registration authentication, the switch needs to obtain the IP address of iMaster NCE-Campus for communication with iMaster NCE-Campus. The switch can obtain the IP address of iMaster NCE-Campus through DHCP or the registration query center or obtain the IP address by resolving the URL configured using the **controller url** command.

Precautions

- If the switch obtains the URL of iMaster NCE-Campus using all the three methods, the URLs are sorted in descending order of priority as follows: URL obtained using DHCP, URL configured using the command, and URL obtained through the registration query center.
- If you run this command multiple times, only the latest configuration takes effect.
- When both the **controller url** command and the **controller ip-address** or **controller backup ip-address** command are configured on the switch, only the latest command takes effect. That is, the switch registers with iMaster NCE-Campus using either the IP address of iMaster NCE-Campus or the IP address resolved from the URL of iMaster NCE-Campus.
- The configuration of this command is saved in the flash memory and therefore cannot be cleared by running the **reset netconf db-configuration** command. To clear the configuration of this command, run the **undo controller url**, **undo netconf**, or **reset factory-configuration** command.

Example

Configure a URL for iMaster NCE-Campus on the switch.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] controller url controller.huawei.com port 10020
```

16.15.13 display netconf alarm active

Function

The **display netconf alarm active** command displays the active alarms reported by the switch to NMS.

Format

display netconf alarm active

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After the NETCONF function is enabled on a switch, you can run the **display netconf alarm active** command to view the active alarms reported by the switch.

Example

Display the active alarms reported by the switch to NMS.

```
<HUAWEI> display netconf alarm active
A/B/C/D/E/F/G
A=Sequence, B=Alarm type, C=Generating time
D=Name, E=Level, F=OID, G=Description

  1/equipmentAlarm/2019-08-27T02:15:42Z/hwPowerInvalid/critical/1.3.6.1.4.1.2011.5.25.219.2.5.5/Power
supply is unavailable for some reason.
(Index=67207181, EntityPhysicalIndex=67207181, PhysicalName="POWER Card 0/PWR2",
EntityTrapFaultID=136973)
  2/equipmentAlarm/2019-08-27T02:15:59Z/hwPowerInvalid/critical/1.3.6.1.4.1.2011.5.25.219.2.5.5/Power
supply is unavailable for some reason.
(Index=68255757, EntityPhysicalIndex=68255757, PhysicalName="POWER Card 1/PWR2",
EntityTrapFaultID=136973)
```

Table 16-87 Description of the **display netconf alarm active** command output

Item	Description
A/B/C/D/E/F/G	Alarm format.
A=Sequence	Alarm sequence number.
B=Alarm type	Alarm type.
C=Generating time	Time when an alarm was generated
D=Name	Alarm name.
E=Level	Alarm severity.
F=OID	Alarm OID.
G=Description	Alarm description.

16.15.14 display netconf configuration

Function

The **display netconf configuration** command displays the information of iMaster NCE-Campus.

Format

display netconf configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the information of iMaster NCE-Campus (such as the IP address), run the **display netconf configuration** command.

This command cannot display the information of iMaster NCE-Campus obtained through DHCP or the registration query center.

Example

Display the information of iMaster NCE-Campus.

```
<HUAWEI> display netconf configuration
---------- Configuration begin----------
controller ip-address 10.1.1.1 port 10020
controller ip-address 192.168.2.2 port 10020 (redirected)
CLI permission: allowed
Current startup rdb file: configbackup/2022-06-23_startup.rdb
---------- Configuration end----------
```

Table 16-88 Description of the **display netconf configuration** command output

Item	Description
controller ip-address 10.1.1.1 port 10020	The configured IP address and port number of iMaster NCE-Campus are 10.1.1.1 and 10020 respectively. If the information is marked with **redirected**, the switch has been redirected from iMaster NCE-Campus with which it just registers to another iMaster NCE-Campus for management.
CLI permission	Whether commands except those for configuring the whitelist can be configured on the device. • denied • allowed (default value) You can change the value only through the iMaster NCE-Campus.
Current startup rdb file	Database file that takes effect currently.

16.15.15 display netconf connect-status

Function

The **display netconf connect-status** command displays the NETCONF configuration on a switch.

Format

display netconf connect-status

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To view the NETCONF configuration on a switch, run the **display netconf connect-status** command.

Example

Display the NETCONF configuration on the switch.

```
<HUAWEI> display netconf connect-status
-------------------------------------------------------------------------------------------------------------
Netconf status               : enable
Upload alarm status          : enable
-------------------------------------------------------------------------------------------------------------
Controller address source    : --
Controller URL               : --
Controller IP address        : --
Controller port              : --
Backup controller URL        : --
Backup controller IP address : 10.1.1.1
Backup controller port       : 10020
Management VLAN              : --
Management IP address        : --
Register phase               : --
Register status              : --
-------------------------------------------------------------------------------------------------------------
Netconf src-ip               : 192.168.10.1
Netconf src-ipv6             : --
Netconf src-port             : 830
Controller information       :
-------------------------------------------------------------------------------------------------------------
No Mode     Name                        IP                   Port  Connected  RegisterStatus
-------------------------------------------------------------------------------------------------------------
1  callhome aa                          192.168.30.1(Master)      10020 N
Unregistered
2  ssh      -                           -                    -     N          -
```

```
3  ssh     -                       -                   -    N        -
------------------------------------------------------------------------------------------------------------
Bootstrap information
  Address source            : User-configured
  Main URL                  : https://1.1.1.1:30217(Active)
  Backup URL                : --
------------------------------------------------------------------------------------------------------------
```

Table 16-89 Description of the **display netconf connect-status** command output

Item	Description
Netconf status	Status of the NETCONF function: ● **enable**: The function is enabled. ● **disable**: The function is disabled. To configure the NETCONF function, run the **netconf** command.
Upload alarm status	Whether the switch is configured to send alarms to the NMS: ● **enable**: The switch is configured to send alarms to the NMS. ● **disable**: The switch cannot send alarms to the NMS.
Controller address source	Source from which the iMaster NCE-Campus address is obtained. ● **User-defined configuration**: indicates that the address is defined by the user. ● **Allocated by Register Center**: indicates that the address is obtained from the registration query center. ● **Allocated by DHCP**: indicates that the address is obtained through DHCP. ● **Allocated by controller**: indicates that the IP address is obtained from iMaster NCE-Campus. ● --: indicates that the iMaster NCE-Campus address is not obtained.
Controller URL	URL of iMaster NCE-Campus. To configure the URL for iMaster NCE-Campus, run the **controller url** command. If no URL is configured or obtained, this parameter value is --.
Controller IP address	IP address of iMaster NCE-Campus. To configure the IP address for iMaster NCE-Campus, run the **controller ip-address** command. If no IP address is configured or obtained, this parameter value is --.

Item	Description
Controller port	Port number of iMaster NCE-Campus. To configure the port number of iMaster NCE-Campus, run the **controller ip-address** command. If no port number is configured or obtained, this parameter value is -.
Backup controller URL	URL of the standby iMaster NCE-Campus. The value can be obtained only through Option 148. If no value is obtained, the parameter value is **--**.
Backup controller IP address	IP address of the standby iMaster NCE-Campus. To configure this parameter, run the **controller backup ip-address** command. If no IP address is configured or obtained, the parameter value is **--**.
Backup controller port	Port number of the standby iMaster NCE-Campus. To configure this parameter, run the **controller backup ip-address** command. If no port number is configured or obtained, the parameter value is **--**.
Management VLAN	Management VLAN ID used when the switch communicates with iMaster NCE-Campus. The management VLAN can be configured using the **management-vlan (NETCONF view)** command. If **Management VLAN (Dynamic)** is displayed in the command output, the management VLAN is automatically negotiated using the PNP protocol. The management VLAN statically configured using the **management-vlan** command in the NETCONF view has a higher priority than the management VLAN dynamically negotiated using PNP.
Management IP address	IP address of the VLANIF interface corresponding to the management VLAN used when the switch communicates with iMaster NCE-Campus. This IP address can be dynamically allocated by the DHCP server, or it can be the static IP address configured for the VLANIF interface corresponding to the management VLAN. If no IP address is dynamically allocated or configured on the VLANIF interface, this parameter value is --.

Item	Description
Register phase	Current registration phase of the switch. ● **DHCP**: The switch is requesting an IP address from a DHCP server. ● **registering**: The switch has obtained an IP address from a DHCP server and is registering with iMaster NCE-Campus. ● **registered**: The switch has registered with iMaster NCE-Campus. ● **aborted**: The process of registering the switch with iMaster NCE-Campus is terminated using the **netconf register abort** command.
Register status	Current registration status of the switch. **NOTE** If the TCP connection between the switch and iMaster NCE-Campus is disconnected, it takes the switch 3 minutes to detect the disconnection. The switch changes from **registered** to **unregistered** state only after detecting the disconnection.
Netconf src-ip	IPv4 address of the switch. To configure the IPv4 address of the switch, run the **source ip** command.
Netconf src-ipv6	IPv6 address of the switch. To configure the IPv6 address of the switch, run the **source ipv6-address** command.
Netconf src-port	Port number used by the switch. To configure the port number, run the **source ip** command.
Controller information	Information about the connected NMS.
No	Connection number.
Mode	NETCONF mode: ● **callhome**: NETCONF over SSH Callhome ● **ssh**: NETCONF over SSH
name	Name of a callhome template. This parameter is not supported in NETCONF over SSH mode and the parameter value will be a hyphen (-) in this mode. To configure the name of a callhome template, run the **callhome** command.
IP	IPv4 address of the NMS. To configure the IPv4 address of the NMS in NETCONF over SSH Callhome mode, run the **ip address** command in the callhome template view.

Item	Description
Port	• This parameter is the port number used by the NMS in NETCONF over SSH Callhome mode. To configure the port number, run the **ip address** command in the callhome template view. • This parameter is the port number used by both the switch and NMS in NETCONF over SSH mode. To configure the port number, run the **source ip** or **source ipv6-address** command.
Connected	Whether the NMS has set up a NETCONF connection with the switch: • **Y**: The NMS has set up a NETCONF connection with the switch. • **N**: The NMS has not set up a NETCONF connection with the switch.
RegisterStatus	Status of the switch on iMaster NCE-Campus. This field is supported only when the NETCONF mode is callhome. • Unregistered: The switch is offline. • Registered: The switch is online. • -: This field is not supported.
Bootstrap information	Bootstrap information.
Address source	Method used to obtain Bootstrap information.
Main URL	Primary address, including the IP address/domain name and port number. If **(Active)** is contained in the value, the device has set up a connection with this address.
Backup URL	Backup address, including the IP address/domain name and port number. If **(Active)** is contained in the value, the device has set up a connection with this address.

16.15.16 display netconf offline-record

Function

The **display netconf offline-record** command displays the reason for the switch to go offline.

Format

display netconf offline-record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a switch goes offline, you can run the **display netconf offline-record** command to check the reason. Only the latest five records will be displayed.

Example

Display the reason for the switch to go offline.

```
<HUAWEI> display netconf offline-record
------------------------------------------------------------------------------
Time                    Error Info
------------------------------------------------------------------------------
2019/10/12 11:13:10     Connect lost
2019/10/12 11:05:53     Connect lost
2019/10/12 10:58:32     Board reset by VRP command or net
manager
2019/10/12 10:58:30     Connect lost
------------------------------------------------------------------------------
```

Table 16-90 Description of the **display netconf offline-record** command output

Item	Description
Time	Time when the switch went offline.

Item	Description
Error Info	Reason for the switch to go offline. • Connect lost • The stackid is inconsistent and setting failed due to fabric port member configuration • Board reset by VRP for unknown reason • Board reset by VRP for registering failure • Board reset by VRP interface management module • Board reset by VRP command or net manager • Board reset by VRP for not ready when slave switching to master • Board reset by VRP for schedule • Board reset by ISSU for switch-prepare or switch-age failed • Board reset by NSR • Board reset by PATCH for restore patch number error • Board reset by PATCH for restore patch file error • Board reset by PATCH for effect after restore running • Board reset by NSF • Board reset by ISIS for purging LSP error • Board reset by OSPF for aging LSA error • Board reset by PATCH for the patch is not empty • Board reset by PATCH for the patch filename or status is incorrect • Board reset by PATCH for the insufficient space or file occupation • Board reset by PATCH for the patch file fails to be synchronized • Board reset by PATCH after the patch is successfully synchronized • Board reset by PATCH due to patch restoration preprocessing failure

16.15.17 display netconf register-fail-record

Function

The **display netconf register-fail-record** command displays records about failed registrations with iMaster NCE-Campus.

Format

display netconf register-fail-record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After this command is executed, a maximum of five registration failure records can be displayed.

If there are multiple registration failures caused by the same reason, only the corresponding registration failure record is updated, which will not overwrite registration failure records with other reasons.

Example

Display records about failed registrations with iMaster NCE-Campus.

```
<HUAWEI> display netconf register-fail-record
--------------------------------------------------------------------------------
Time                    Error Info
--------------------------------------------------------------------------------
2019/11/09 23:21:02     Failed to apply IP address
2019/11/09 23:12:13     Failed to create TCP link to controller (192.168.1.1)
2022/07/09 22:21:02     Failed to obtain the Lite CA certificate from the bootstrap server
2022/09/09 22:21:02     Failed to obtain local certificate (192.168.1.1)
--------------------------------------------------------------------------------
```

Table 16-91 Description of the **display netconf register-fail-record** command output

Item	Description
Time	Registration failure time.

Item	Description
Error Info	Reason for the registration failure. The IP address in this parameter value is the IP address of iMaster NCE-Campus with which the switch failed to register. Possible reasons are as follows: • Manage VLAN is physical down • Change to tradition work mode failed • Failed to apply IP address • No DNS information in DHCP options • No controller IP or URL information • Failed to get IP address of controller • Failed to create TCP link to controller • Failed to get register result from controller • Controller certificate authentication failed • Controller ESN check failed • Device is not authorized • Device type and ESN does not match • Failed to connect registration center • The configuration of the device is inconsistent with that of the controller: For example, the stack configuration exists on the device, but not on the controller. • The slot number of the device is inconsistent with that on the controller • The controller failed to verify the sitecode • Failed to obtain the Lite CA certificate from the bootstrap server • Failed to obtain local certificate • Others

16.15.18 display netconf { rsa | dsa } local-key-pair public

Function

The **display netconf { rsa | dsa } local-key-pair public** command displays the public key in the local RSA or DSA key pair.

Format

display netconf { rsa | dsa } local-key-pair public

Parameters

Parameter	Description	Value
rsa	Displays the public key in the local RSA key pair.	-
dsa	Displays the public key in the local DSA key pair.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to display the public key in the RSA or DSA key pair on a switch, and then copy the public key to the RSA or DSA public key on the controller. In this way, the public keys on the switch and controller are the same, ensuring successful authentication.

Example

Display the public key in the local DSA key pair.

```
<HUAWEI> display netconf dsa local-key-pair public
The DSA public key:
ssh-dss AAAAB3NzaC1kc3MAAACBAOAWWAtGClBH4qhgm0+ntDTZVW/tR8R9Vn
+rXVA8GFWM5TVUJWXFWghy4QTJqmvg+ca0znn+c2hDGDhx1yhRsduKWmOBAzIQE/
1OYhMLdK0vRmceyYtSTfVNCbtAwJNOM0JPBlbim/
vjp3aX3iRn6EPU7bYaJ3A8KEUZlVKh7YU5AAAAFQCQ8znriZRmpyoAVK68YPNDnKzkGQAAAIA8f1ELwIJC9J73z
g6an2Hz7P3zDAqDv2mnvOuvKEbVWY3IVNhCHaX39yBl0PT2rWmXzHI6nJWEPiuoW/
eJpDxNwV1OCgSN4mhG90/
iOJkLKqF6UENdQWXNKbjLHYKTkKXSnpi2ibqEzrqnbkzIVbaf2a8nBDrh1CHKRhw1dQChggAAAIA7TGIupodUc1
Enn3rzTNch5rL0CKL9znjFG+lyeJU39fDWSOVfgWfz4ehs48/5Zco6H9wj1seLxh3pVXYLqJvRDR6B0g/
68T3aEYEKGoHeRYC3sU80lXb8s0VFae90ohOf89ULyfVt7HVE+QKkExQIj9sAo8KbR3gNkb84PM+Z9g==
root@root
```

16.15.19 display work-mode

Function

The **display work-mode** command displays the working mode of the switch.

Format

display work-mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display work-mode** command to view the working mode of a switch.

Example

Display the working mode of the switch.

```
<HUAWEI> display work-mode
Current work-mode       : NETCONF
Work-mode before upgrade: Cloud-mng
```

Table 16-92 Description of the **display work-mode** command output

Item	Description
Current work-mode	Working mode of the switch: ● NETCONF: NETCONF is enabled. ● Tradition: NETCONF is disabled.
Work-mode before upgrade	Working mode of the switch before the upgrade. **Cloud-mng** indicates cloud-based management. This field is displayed only when a switch working in cloud-based management mode is upgraded to V200R019C00 or a later version.

16.15.20 ip address (callhome template view)

Function

The **ip address** command configures the IPv4 address and port number used by the NMS that communicates with a switch through NETCONF.

The **undo ip address** command deletes the IPv4 address and port number used by the NMS that communicates with a switch through NETCONF.

By default, no IPv4 address and port number have been configured for the NMS with which the switch communicates through NETCONF.

Format

ip address *ip-address* **port** *port-number*

undo ip address

Parameters

Parameter	Description	Value
ip-address	IPv4 address of the NMS.	The value is in dotted decimal notation.
port *port-number*	Port number used by the NMS.	The value is an integer in the range 1 to 65535.

Views

Callhome template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS needs to configure and manage a switch in NETCONF over SSH Callhome mode, you must run the **ip address** command to configure the IPv4 address and port number for the NMS so that the switch can proactively set up a NETCONF connection with the NMS.

Precautions

If a switch that has registered with a iMaster NCE-Campus needs to register with another iMaster NCE-Campus, restart the switch before the re-registration.

Example

Set the IP address and port number used by the NMS to communicate with the switch through NETCONF to 10.1.2.1 and 10020, respectively.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] callhome Test123
[HUAWEI-netconf-callhome-Test123] ip address 10.1.2.1 port 10020
```


16.15.21 lldp tlv-enable legacy-tlv pnp

Function

The **lldp tlv-enable legacy-tlv pnp** command configures an interface to advertise PnP TLVs.

The **undo lldp tlv-enable legacy-tlv pnp** command disables an interface from advertising PnP TLVs.

By default, an interface advertises all PnP TLVs.

Format

lldp tlv-enable legacy-tlv pnp { **all** | **startup-vlan** | **startup-link-aggregation** | **device-type** }

undo lldp tlv-enable legacy-tlv pnp { **all** | **startup-vlan** | **startup-link-aggregation** | **device-type** }

Parameters

Parameter	Description	Value
all	Advertises all PnP TLVs.	-
startup-vlan	Specifies the PnP TLVs to be advertised to VLAN IDs.	-
startup-link-aggregation	Specifies the PnP TLVs to be advertised to the Eth-Trunk flag and LACP mode flag.	-
device-type	Specifies the PnP TLVs to be advertised to device types.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, 25GE interface view, port group view

Default Level

2: Configuration level

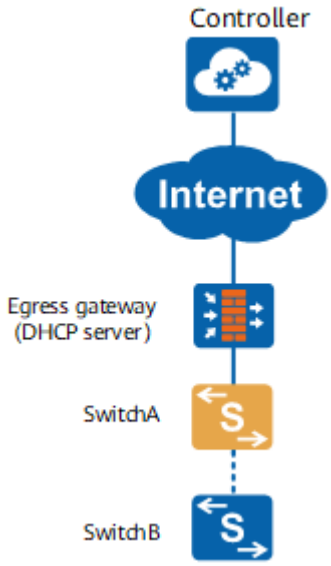
Usage Guidelines

- **Scenario 1: All switches on a CloudCampus network can be managed by iMaster NCE-Campus.**

  On the CloudCampus network shown in **Figure 16-2**, SwitchA and SwitchB are both switches. SwitchB is newly connected to the network when the VLAN

for the IP address pool of the DHCP server is not VLAN 1. After SwitchB is connected to the network, by default, it uses the management VLAN 1 to send a request packet to the DHCP server to obtain the NETCONF enabling configuration, IP address, and information of iMaster NCE-Campus. However, SwitchB fails to obtain the information because the VLAN for the IP address pool of the DHCP server is not VLAN 1.

Figure 16-2 CloudCampus networking



To address the problem, configure PnP VLAN auto-negotiation on SwitchA. After SwitchB starts, SwitchA transmits the PnP VLAN ID to SwitchB through PnP VLAN auto-negotiation, so that SwitchB can use the PnP VLAN to obtain related information from the DHCP server.

SwitchA can transmit the PnP VLAN ID to SwitchB only when SwitchA meets the following conditions:

- SwitchA has registered with iMaster NCE-Campus successfully.
- iMaster NCE-Campus has delivered a PnP VLAN ID to SwitchA, and the configuration file contains the **pnp startup-vlan** *vlan-id* command or SwitchA has negotiated a PnP VLAN ID with its upstream device.
- iMaster NCE-Campus has delivered the function of transmitting the PnP VLAN ID to the downstream device to SwitchA, and the configuration file contains the **pnp startup-vlan send enable** command.
- SwitchA is enabled to send LLDPDUs containing PnP VLAN information to its downstream device. This function is enabled by default. If the configuration file contains the **undo lldp tlv-enable legacy-tlv pnp startup-vlan** or **undo lldp tlv-enable legacy-tlv pnp all** command, the function of sending LLDPDUs containing the PnP VLAN ID to the downstream device is disabled. You can enable the function on iMaster NCE-Campus.

SwitchB can obtain the PnP VLAN ID transmitted by SwitchA only after SwitchB is enabled to receive the PnP VLAN negotiation packets sent by its upstream device. This function is enabled by default. If the configuration file contains the **undo pnp startup-vlan receive enable** command, the function

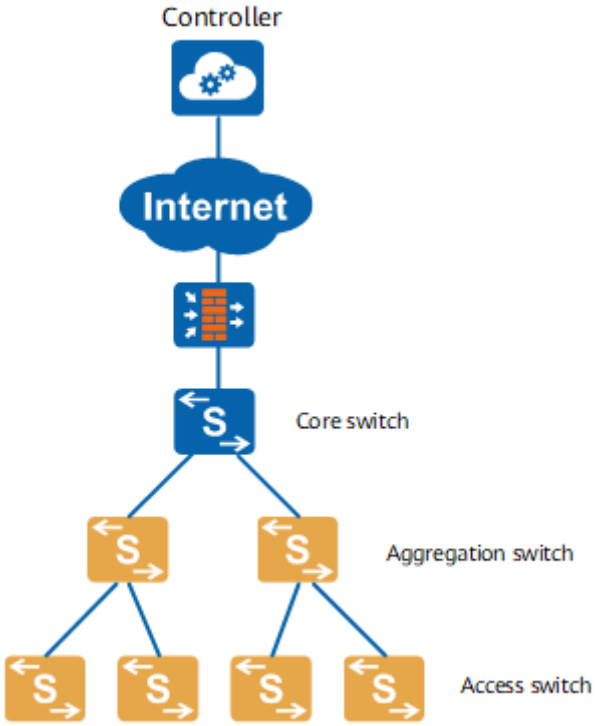
of receiving the PnP VLAN negotiation packets sent by the upstream device is disabled. You can enable the function on iMaster NCE-Campus.

The function of transmitting the PnP VLAN ID to the downstream device and the PnP VLAN ID can be preconfigured on iMaster NCE-Campus and delivered to a switch after the switch has registered with iMaster NCE-Campus.

- **Scenario 2: On a CloudCampus network, some switches cannot be managed by iMaster NCE-Campus.**

  On the CloudCampus network shown in **Figure 16-3**, the access and aggregation switches can be managed by iMaster NCE-Campus. The core switch is not managed by iMaster NCE-Campus. When the management VLAN is changed on iMaster NCE-Campus from VLAN 1 (default) to VLAN 2, the core switch needs to notify its downstream switches of the new management VLAN ID.

  Figure 16-3 CloudCampus networking

  Configure PnP VLAN auto-negotiation on the core switch so that the core switch can notify its downstream switches of the new management VLAN ID. This process consists of the following operations:

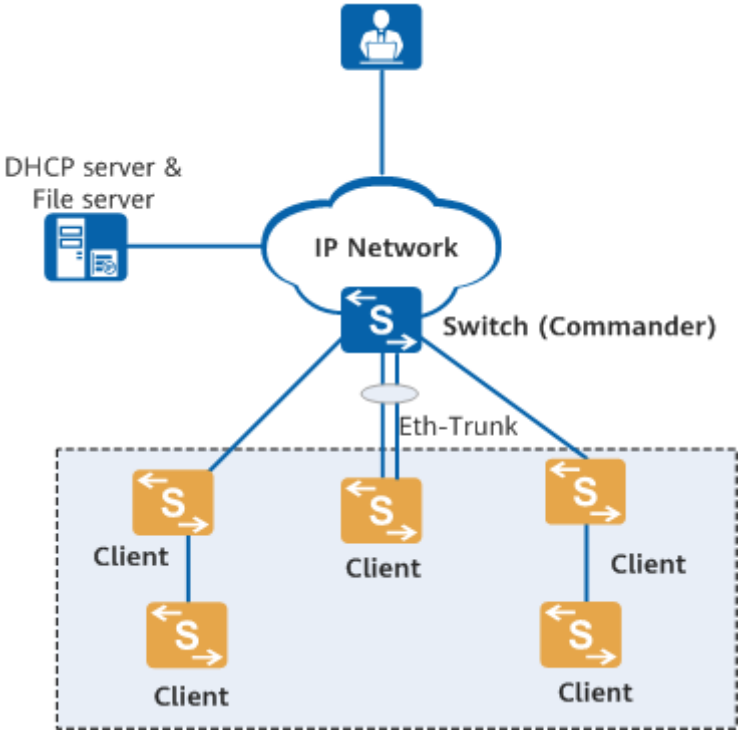
  - Run the **pnp startup-vlan** command to configure a PnP VLAN ID.
  - Run the **pnp startup-vlan send enable** command to enable the switch to transmit the PnP VLAN ID to its downstream devices.
  - Run the **lldp tlv-enable legacy-tlv pnp all** command to enable the device to send LLDPDUs containing PnP information to its downstream devices. This function is enabled by default. LLDPDUs carry PnP information, including the PnP VLAN ID, Eth-Trunk enabling flag, LACP mode flag, and device type.
  - If the core switch and the aggregation switches are connected through Eth-Trunks, you also need to run the **pnp startup-link-aggregation**

enable command to enable the function of notifying downstream devices of the need to establish an Eth-Trunk. After the command is run, the downstream devices will automatically add interfaces to Eth-Trunks based on the negotiation. LLDPDUs carry the Eth-Trunk enabling flag and LACP mode flag.

- **Scenario 3: Zero-touch deployment using EasyDeploy**

  In **Figure 16-4**, when EasyDeploy is used for zero touch deployment, the Commander needs to notify a client of the new VLAN ID if the Commander does not use VLAN 1 to communicate with the client.

  Figure 16-4 EasyDeploy networking diagram



- Configure PnP VLAN auto-negotiation on the Commander to enable the Commander to notify clients of the new VLAN ID. This process consists of the following operations:
  - Run the **pnp startup-vlan** command to configure a PnP VLAN ID.
  - Run the **pnp startup-vlan send enable** command to enable the switch to transmit the PnP VLAN ID to its downstream devices.
  - Run the **lldp tlv-enable legacy-tlv pnp all** command to enable the device to send LLDPDUs containing PnP information to its downstream devices. This function is enabled by default. LLDPDUs carry PnP information, including the PnP VLAN ID, Eth-Trunk enabling flag, LACP mode flag, and device type.
  - If the core switch and the aggregation switches are connected through Eth-Trunks, you also need to run the **pnp startup-link-aggregation enable** command to enable the function of notifying downstream devices of the need to establish an Eth-Trunk. After the command is run, the downstream devices will automatically add interfaces to Eth-Trunks based on the negotiation. LLDPDUs carry the Eth-Trunk enabling flag and LACP mode flag.

Example

Enable a switch to send LLDPDUs containing PnP VLAN information to downstream devices.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] lldp tlv-enable legacy-tlv pnp startup-vlan
```

16.15.22 management-vlan (NETCONF view)

Function

The **management-vlan** command configures the VLAN used by the switch to communicate with a DHCP server. This VLAN is the management VLAN of the switch.

Format

management-vlan *vlan-id*

undo management-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID used by the switch to communicate with a DHCP server.	The value is an integer in the range 1 to 4094.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In NETCONF over SSH Callhome mode, the switch can obtain the IP address of iMaster NCE-Campus using DHCP. The request sent by the switch to the DHCP server to obtain the IP address of iMaster NCE-Campus is transmitted over VLAN 1. After the switch passes registration authentication, iMaster NCE-Campus changes the VLAN ID used by the switch to communicate with the DHCP server again. After the switch restarts, to ensure that it continues to use the configured VLAN to communicate with the DHCP server, you can configure the management VLAN on the switch.

Precautions

- This command cannot be configured if the **source ip-address** command has been executed in the SMI view to configure the IPv4 address used by the switch to communicate with the NMS (such as the analyzer iMaster NCE-CampusInsight).
- The management VLAN of the switch cannot be the same as the management VLAN of the CAPWAP tunnel.
- When you disable NETCONF in the system view or delete the management VLAN in the NETCONF view, the system displays a message asking you whether to retain the **ip address dhcp-alloc** configuration. Exercise caution when you choose to delete the configuration.
- Assume that a static IP address has been configured for a VLANIF interface. When you run the **management-vlan** command to configure the VLAN corresponding to this VLANIF interface as the management VLAN, the device displays a message indicating that users in the management VLAN will be unable to go online through DHCP. Exercise caution when running this command.

Example

Set the management VLAN ID of the switch to 2.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] management-vlan 2
```

16.15.23 netconf

Function

The **netconf** command enables the NETCONF function and enters the NETCONF view.

The **undo netconf** command disables the NETCONF function.

By default, NETCONF is disabled on a switch.

Format

netconf

undo netconf

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS needs to configure and manage a switch using NETCONF, run the **netconf** command on the switch to enable the NETCONF function.

Precautions

- After the **undo netconf** command is executed on the switch to disable the NETCONF function, all NETCONF configurations, all the database information, and the **card register-permit** configuration on the switch are deleted, leading to communication interruption between the switch and NMS.
- Before running the **netconf** command to enable the NETCONF function, ensure that port 830 and ports 55552 to 55807 are not in use. Otherwise, NETCONF cannot be enabled.
- Before running the **netconf** command to enable the NETCONF function, ensure that the fixed IP address 169.254.2.1 that is automatically configured for a virtual management interface is not in use. Otherwise, NETCONF cannot be enabled.
- If Eth-Trunk 0 has been created on a switch, Eth-Trunk auto-negotiation will become abnormal after you enable the NETCONF function using the **netconf** command.
- When you disable NETCONF in the system view or delete the management VLAN in the NETCONF view, the system will prompt you to delete the **ip address dhcp-alloc** configuration. Exercise caution when you choose to delete the configuration.
- For the S6735-S, S6720-EI and S6720S-EI, when you run the **netconf** command to enable NETCONF, the device automatically delivers the **unknown-unicast load-balance enhanced lbid** command and displays a message indicating that enabling NETCONF will automatically disable LNP, enable STP, and configure load balancing for broadcast, unknown unicast, and multicast packets (BUM packets). Exercise caution when performing this operation. If the S6735-S, S6720-EI or S6720S-EI running a version earlier than V200R021C10 is enabled with NETCONF and then is upgraded to V200R021C10 or later, the switch does not automatically deliver the **unknown-unicast load-balance enhanced lbid** command for upgrade compatibility purposes.

Example

Enable the NETCONF function and display the NETCONF view.

```
<HUAWEI> system-view
[HUAWEI] netconf
```

16.15.24 netconf config enhanced

Function

The **netconf config enhanced** command sets the configuration mode of a switch to enhanced mode.

The **undo netconf config enhanced** command restores the default configuration mode of a switch.

By default, the default configuration mode is used on a switch.

Format

netconf config enhanced

undo netconf config enhanced

Parameters

None

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

When the default configuration mode is used on a switch, the switch limits the number of objects in the packets sent from iMaster NCE-Campus. If the number of objects in the packets sent from iMaster NCE-Campus exceeds this limit, the switch returns an error message indicating that the configuration fails to be delivered.

To remove this limit, run the **netconf config enhanced** command on the switch to enable the enhanced configuration mode.

In versions earlier than V200R022C10, a switch does not limit the number of nodes in packets issued by iMaster NCE-Campus packets. After the switch is upgraded to V200R022C10 or a later version, the **netconf config enhanced** configuration is automatically added to the configuration file to ensure that the switch still has no such a limitation after the upgrade.

NOTICE

The enhanced configuration mode of a switch affects system stability, which may cause device exceptions. Therefore, use this function under the guidance of technical support engineers.

Example

Set the switch configuration mode to default mode.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] undo netconf config enhanced
```


16.15.25 netconf alarm upload enable

Function

The **netconf alarm upload enable** command enables the switch to report alarms to the NMS.

The **undo netconf alarm upload enable** command disables the switch from reporting alarms to the NMS.

By default, a switch is enabled to report alarms to the NMS.

Format

netconf alarm upload enable

undo netconf alarm upload enable

Parameters

None

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

If a switch reports a large number of alarms to the NMS, the CPU usage of the switch is high. As a result, services cannot be configured on the switch. To prevent this problem, you can run the **undo netconf alarm upload enable** command to disable the device from reporting alarms to the NMS.

Example

Disable the device from reporting alarms to the NMS.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] undo netconf alarm upload enable
```

16.15.26 netconf register abort

Function

The **netconf register abort** command terminates a switch's registration with iMaster NCE-Campus.

The **undo netconf register abort** command resumes a switch's registration with iMaster NCE-Campus.

By default, a switch registers with iMaster NCE-Campus normally.

Format

netconf register abort

undo netconf register abort

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a switch fails to register with iMaster NCE-Campus, log in to the switch through SSH to view the registration status. If the registration process is not terminated, the DHCP server may re-assign an IP address to the switch, which will cause the SSH login process to terminate. To prevent this problem, log in to the switch and then run the **netconf register abort** command to terminate the registration process.

After this command is executed, the registration process stops for 30 minutes and then resumes. To view the registration status, run the **display netconf connect-status** command.

Precautions

- The **netconf register abort** command cannot be executed repeatedly.
- Do not run this command when the switch has registered with iMaster NCE-Campus successfully.
- The command configuration is not recorded to the configuration file and the command will become ineffective after the switch restarts.
- If this command is run and iMaster NCE-Campus displays the device status as registered, the actual registration status is subject to the **display netconf connect-status** command output.

Example

Terminate the switch's registration with iMaster NCE-Campus.

```
<HUAWEI> system-view
[HUAWEI] netconf register abort
```


16.15.27 pnp disable

Function

The **pnp disable** command disables PnP negotiation on an interface.

The **undo pnp disable** command enables PnP negotiation on an interface.

By default, PnP negotiation is enabled on an interface of a switch.

Format

pnp disable

undo pnp disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, 100GE interface view, 25GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a campus solution scenario, newly connected switches can go online through a PnP VLAN. By default, PnP negotiation is enabled on interfaces. If a new downstream access switch is planned not to use a PnP VLAN to register with and go online on iMaster NCE-Campus, you can disable PnP negotiation on the interface connected to the downstream switch.

Precautions

This command cannot be configured in the Eth-Trunk 0 interface view.

Example

Disable PnP on an interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] pnp disable
```


16.15.28 pnp startup-link-aggregation enable

Function

The **pnp startup-link-aggregation enable** command enables a switch to inform its downstream device of the need to establish an Eth-Trunk.

The **undo pnp startup-link-aggregation enable** command disables a switch from informing its downstream device of the need to establish an Eth-Trunk.

By default, a switch is disabled from informing its downstream device of the need to establish an Eth-Trunk.

Format

pnp startup-link-aggregation enable

undo pnp startup-link-aggregation enable

Parameters

None

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Figure 16-5 CloudCampus network diagram

As shown in **Figure 16-5**, the new switch, SwitchB, is connected to its upstream device, SwitchA, through two links. When SwitchB and SwitchA negotiate the PnP VLAN, if SwitchA is enabled to inform its downstream device of the need to establish an Eth-Trunk, SwitchB adds two links to the Eth-Trunk and sets the Eth-Trunk mode based on whether the Eth-Trunk mode of SwitchA is LACP.

The auto-negotiated Eth-Trunk can only be Eth-Trunk0, which is reserved on iMaster NCE-Campus and cannot be used by other services.

Precautions

- Running this command on uplink interfaces is not recommended, as it will cause connection failures.
- Only the following configurations are allowed on the physical uplink port of the downstream device when this port is added to Eth-Trunk 0 through auto-negotiation. If any other configurations exist on the physical uplink port, it cannot be automatically added to Eth-Trunk 0.
  - **trust dscp**
  - **port link-type trunk**
  - **description** *description*
- After a switch registers with iMaster NCE-Campus, you are advised to fix the auto-negotiated Eth-Trunk through iMaster NCE-Campus. This prevents the configuration from becoming invalid after the switch goes offline from the controller.

Example

Enable the function of transmitting the flag indicating whether to establish an Eth-Trunk to downstream devices.


```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] pnp startup-link-aggregation enable
```

16.15.29 pnp startup-link-aggregation receive enable

Function

The **pnp startup-link-aggregation receive enable** command enables Eth-Trunk auto-negotiation.

The **undo pnp startup-link-aggregation receive enable** command disables Eth-Trunk auto-negotiation.

By default, Eth-Trunk auto-negotiation is enabled.

Format

pnp startup-link-aggregation receive enable

undo pnp startup-link-aggregation receive enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device goes online through a negotiated PnP VLAN and the network of the upstream device becomes stable, you can run the **undo pnp startup-link-aggregation receive enable** command on the downstream device to disable Eth-Trunk auto-negotiation. Then, the device will not accept new Eth-Trunk auto-negotiation requests. In this way, the configuration of Eth-Trunk 0 and its member interfaces remain unchanged, preventing flapping of the upstream device from affecting local services. If Eth-Trunk auto-negotiation is not disabled, the connection between the device and controller will be unstable when Eth-Trunk members are added or deleted.

Precautions

After Eth-Trunk auto-negotiation is disabled, if the networking mode of the upstream device changes, you need to enable Eth-Trunk auto-negotiation again.

Example

Disable Eth-Trunk auto-negotiation.


```
<HUAWEI> system-view
[HUAWEI] undo pnp startup-link-aggregation receive enable
```

16.15.30 pnp startup-vlan

Function

The **pnp startup-vlan** command configures a wired PnP VLAN ID for wired devices.

The **undo pnp startup-vlan** command deletes a wired PnP VLAN ID.

By default, no wired PnP VLAN ID is configured on a switch.

Format

pnp startup-vlan *vlan-id*

undo pnp startup-vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies a wired PnP VLAN ID.	The value is an integer in the range 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

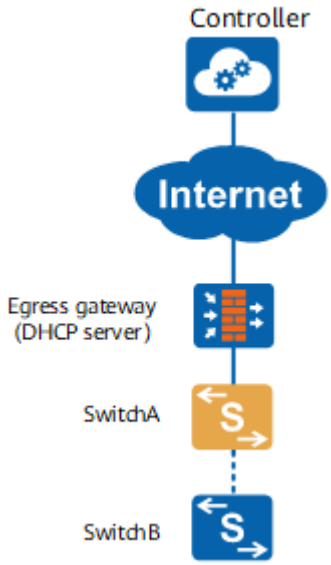
There are two types of PnP VLANs: wired and wireless PnP VLANs. Switches obtain management IP addresses through the wired PnP VLAN. When a switch has APs connected, the switch automatically changes the PVID of interfaces connected to the APs to the wireless PnP VLAN ID. For switches, PnP VLAN negotiation involves both wired and wireless PnP VLANs. The PnP VLAN applies to the following scenarios:

- **Scenario 1: All switches on a CloudCampus network can be managed by iMaster NCE-Campus.**

  On the CloudCampus network shown in **Figure 16-6**, SwitchA and SwitchB are both switches. SwitchB is newly connected to the network when the VLAN for the IP address pool of the DHCP server is not VLAN 1. After SwitchB is connected to the network, by default, it uses the management VLAN 1 to send a request packet to the DHCP server to obtain the NETCONF enabling

configuration, IP address, and information of iMaster NCE-Campus. However, SwitchB fails to obtain the information because the VLAN for the IP address pool of the DHCP server is not VLAN 1.

Figure 16-6 CloudCampus networking



To address the problem, configure PnP VLAN auto-negotiation on SwitchA. After SwitchB starts, SwitchA transmits the PnP VLAN ID to SwitchB through PnP VLAN auto-negotiation, so that SwitchB can use the PnP VLAN to obtain related information from the DHCP server.

SwitchA can transmit the PnP VLAN ID to SwitchB only when SwitchA meets the following conditions:

- SwitchA has registered with iMaster NCE-Campus successfully.
- iMaster NCE-Campus has delivered a PnP VLAN ID to SwitchA, and the configuration file contains the **pnp startup-vlan** *vlan-id* command or SwitchA has negotiated a PnP VLAN ID with its upstream device.
- iMaster NCE-Campus has delivered the function of transmitting the PnP VLAN ID to the downstream device to SwitchA, and the configuration file contains the **pnp startup-vlan send enable** command.
- SwitchA is enabled to send LLDPDUs containing PnP VLAN information to its downstream device. This function is enabled by default. If the configuration file contains the **undo lldp tlv-enable legacy-tlv pnp startup-vlan** or **undo lldp tlv-enable legacy-tlv pnp all** command, the function of sending LLDPDUs containing the PnP VLAN ID to the downstream device is disabled. You can enable the function on iMaster NCE-Campus.

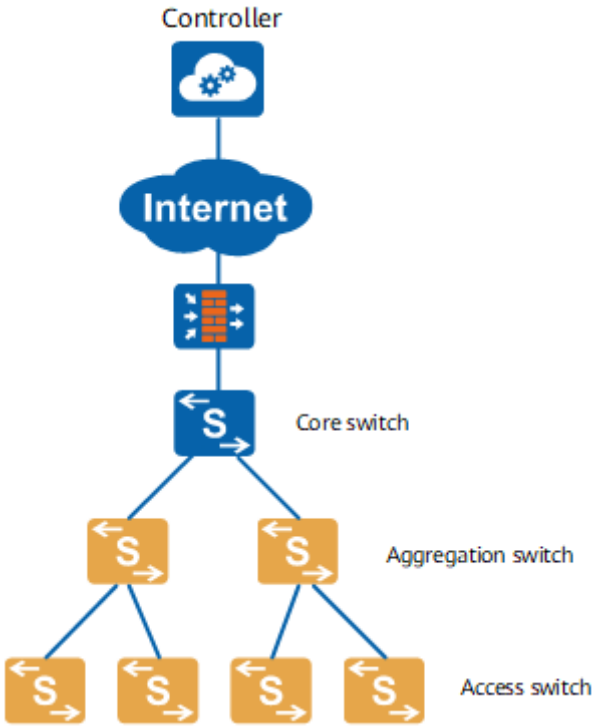
SwitchB can obtain the PnP VLAN ID transmitted by SwitchA only after SwitchB is enabled to receive the PnP VLAN negotiation packets sent by its upstream device. This function is enabled by default. If the configuration file contains the **undo pnp startup-vlan receive enable** command, the function of receiving the PnP VLAN negotiation packets sent by the upstream device is disabled. You can enable the function on iMaster NCE-Campus.

The function of transmitting the PnP VLAN ID to the downstream device and the PnP VLAN ID can be preconfigured on iMaster NCE-Campus and delivered to a switch after the switch has registered with iMaster NCE-Campus.

- **Scenario 2: On a CloudCampus network, some switches cannot be managed by iMaster NCE-Campus.**

  On the CloudCampus network shown in **Figure 16-7**, the access and aggregation switches can be managed by iMaster NCE-Campus. The core switch is not managed by iMaster NCE-Campus. When the management VLAN is changed on iMaster NCE-Campus from VLAN 1 (default) to VLAN 2, the core switch needs to notify its downstream switches of the new management VLAN ID.

  Figure 16-7 CloudCampus networking



  Configure PnP VLAN auto-negotiation on the core switch so that the core switch can notify its downstream switches of the new management VLAN ID. This process consists of the following operations:

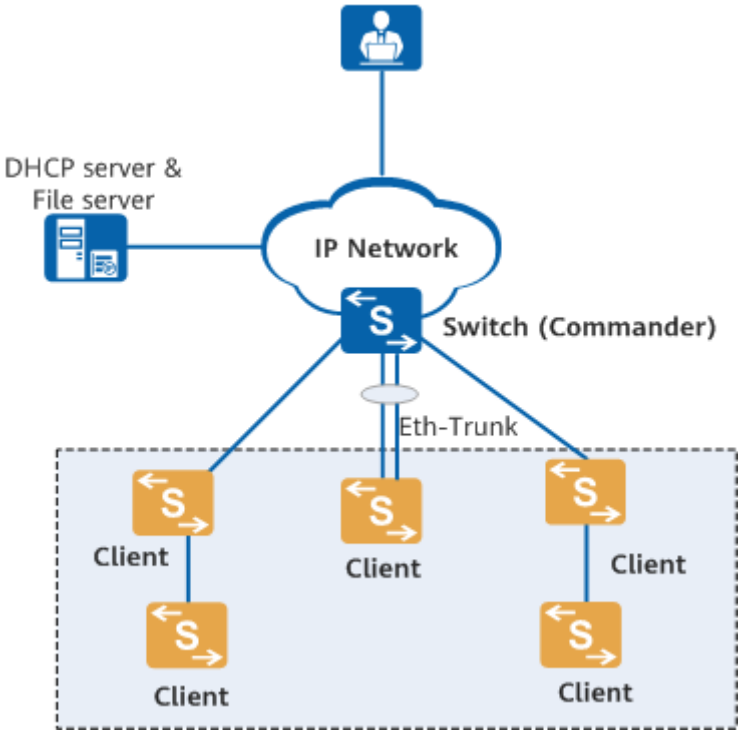
  - Run the **pnp startup-vlan** command to configure a PnP VLAN ID.
  - Run the **pnp startup-vlan send enable** command to enable the switch to transmit the PnP VLAN ID to its downstream devices.
  - Run the **lldp tlv-enable legacy-tlv pnp all** command to enable the device to send LLDPDUs containing PnP information to its downstream devices. This function is enabled by default. LLDPDUs carry PnP information, including the PnP VLAN ID, Eth-Trunk enabling flag, LACP mode flag, and device type.
  - If the core switch and the aggregation switches are connected through Eth-Trunks, you also need to run the **pnp startup-link-aggregation enable** command to enable the function of notifying downstream devices

of the need to establish an Eth-Trunk. After the command is run, the downstream devices will automatically add interfaces to Eth-Trunks based on the negotiation. LLDPDUs carry the Eth-Trunk enabling flag and LACP mode flag.

- **Scenario 3: Zero-touch deployment using EasyDeploy**

  In **Figure 16-8**, when EasyDeploy is used for zero touch deployment, the Commander needs to notify a client of the new VLAN ID if the Commander does not use VLAN 1 to communicate with the client.

  Figure 16-8 EasyDeploy networking diagram



- Configure PnP VLAN auto-negotiation on the Commander to enable the Commander to notify clients of the new VLAN ID. This process consists of the following operations:
  - Run the **pnp startup-vlan** command to configure a PnP VLAN ID.
  - Run the **pnp startup-vlan send enable** command to enable the switch to transmit the PnP VLAN ID to its downstream devices.
  - Run the **lldp tlv-enable legacy-tlv pnp all** command to enable the device to send LLDPDUs containing PnP information to its downstream devices. This function is enabled by default. LLDPDUs carry PnP information, including the PnP VLAN ID, Eth-Trunk enabling flag, LACP mode flag, and device type.
  - If the core switch and the aggregation switches are connected through Eth-Trunks, you also need to run the **pnp startup-link-aggregation enable** command to enable the function of notifying downstream devices of the need to establish an Eth-Trunk. After the command is run, the downstream devices will automatically add interfaces to Eth-Trunks based on the negotiation. LLDPDUs carry the Eth-Trunk enabling flag and LACP mode flag.

Precautions

- If the management VLAN of a switch is set to VLAN 1 through iMaster NCE-Campus or a command, the switch automatically goes online in the PNP VLAN. If the management VLAN configured through iMaster NCE-Campus or a command is not VLAN 1, the switch uses the management VLAN to send a request to the DHCP server. Even if the request fails, the switch does not use the PNP VLAN to send a request to the DHCP server. Therefore, ensure that the switch can communicate with the DHCP server through the management VLAN. Otherwise, the switch cannot go online.
- The wired PnP VLAN must have been created and cannot be the reserved VLAN of a stack, the control VLAN of RRPP/ERPS/SEP or the management VLAN of a CAPWAP tunnel in an SVF system.
- The wired and wireless PnP VLANs can be the same or different.
- If a wired PnP VLAN is configured and no wireless PnP VLAN is configured (using the **pnp wireless startup-vlan** command), the PVID of the interface connecting the switch to an AP is changed to the wired PnP VLAN.

Example

Configure the PnP VLAN ID.

```
<HUAWEI> system-view
[HUAWEI] pnp startup-vlan 2
```

16.15.31 pnp wireless startup-vlan

Function

The **pnp wireless startup-vlan** command configures a wireless PnP VLAN ID for APs.

The **undo pnp wireless startup-vlan** command deletes a wireless PnP VLAN ID.

By default, no wireless PnP VLAN ID is configured on a switch.

Format

pnp wireless startup-vlan *vlan-id*

undo pnp wireless startup-vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies a wireless PnP VLAN ID.	The value is an integer in the range 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a smart campus network, wired devices (such as switches) and wireless devices (such as APs) can use different management VLANs to facilitate maintenance and management. The wired and wireless devices can obtain management VLANs through the wired and wireless PnP VLANs, respectively.

- When all devices on the network can be managed by iMaster NCE-Campus, you can pre-configure wired and wireless PnP VLANs on iMaster NCE-Campus. After switches successfully register with iMaster NCE-Campus, iMaster NCE-Campus automatically delivers the wired and wireless PnP VLANs to the switches. When a switch identifies that the downstream device is an AP, it automatically changes the PVID of the interface connected to the AP to the wireless PnP VLAN ID and add the interface to the wireless PnP VLAN ID .
- If some switches on the network cannot be managed by iMaster NCE-Campus, you can manually configure wired and wireless PnP VLANs on these switches, which will deliver the PnP VLANs to downstream devices.

The device can obtain a wireless PnP VLAN in multiple ways. A wireless PnP VLAN configured using a command takes precedence over that negotiated with the upstream device. If no wireless PnP VLAN is specified or negotiated with the upstream devices, a wired PnP VLAN is used as a wireless PnP VLAN. To be specific, the device determines the PnP VLAN to be used as the wireless PnP VLAN in descending order of priority as follows:

1. Wireless PnP VLAN configured using the **pnp wireless startup-vlan** command
2. Wired PnP VLAN configured using the **pnp startup-vlan** command
3. Wireless PNP VLAN negotiated with the upstream device
4. Wired PnP VLAN negotiated with the upstream device

Precautions

- The VLAN used as the wireless PnP VLAN must have been created and cannot be the reserved VLAN of a stack, the control VLAN of RRPP/ERPS/SEP, or the management VLAN of a CAPWAP tunnel in an SVF system.
- The wired and wireless PnP VLANs can be the same or different.
- When a switch identifies that the downstream device is an AP, the switch adds the interconnection interface to the PnP VLAN. However, no corresponding configuration is added to the configuration file, and this interface cannot be removed from the PnP VLAN by manually adding the interface to the PnP VLAN and then removing the interface from the PnP VLAN.
- If a wired PnP VLAN is configured and no wireless PnP VLAN is configured (using the **pnp wireless startup-vlan** command), the PVID of the interface connecting the switch to an AP is changed to the wired PnP VLAN.

Example

Configure a wireless PnP VLAN ID.

```
<HUAWEI> system-view
[HUAWEI] pnp wireless startup-vlan 2
```

16.15.32 pnp startup-vlan receive enable

Function

The **pnp startup-vlan receive enable** command enables a switch to receive the PnP VLAN negotiation packets sent by its upstream device.

The **undo pnp startup-vlan receive enable** command disables a switch from receiving the PnP VLAN negotiation packets sent by its upstream device.

By default, a switch is enabled to receive the PnP VLAN negotiation packets from its upstream device.

Format

pnp startup-vlan receive enable

undo pnp startup-vlan receive enable

Parameters

None

Views

System view

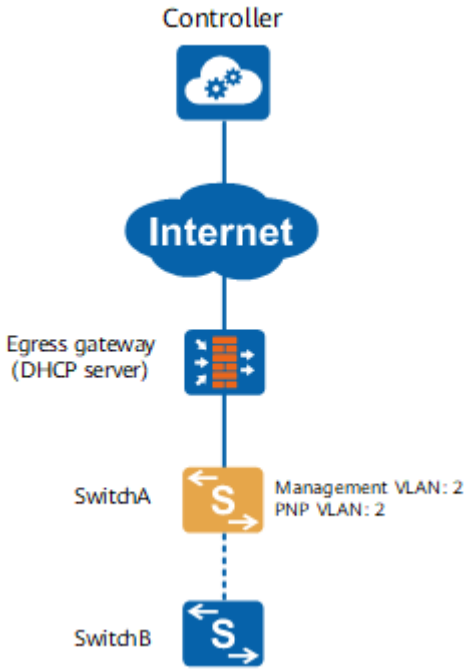
Default Level

2: Configuration level

Usage Guidelines

On a campus network shown in **Figure 16-9**, the VLAN for the IP address pool of the DHCP server is not VLAN 1 and SwitchB is newly connected to the network. After SwitchB is connected to the network, it uses the management VLAN 1 to send a request packet to the DHCP server to obtain the NETCONF enabling configuration, IP address, and information of controller. The VLAN for the IP address pool of the DHCP server is not VLAN 1. As a result, SwitchB cannot obtain the related information.

Figure 16-9 Campus network diagram



To address the problem, configure PnP VLAN auto-negotiation on SwitchA. After SwitchB starts, SwitchA transmits the PnP VLAN ID to SwitchB through PnP VLAN auto-negotiation, so that SwitchB can use the PnP VLAN to obtain the related information from the DHCP server.

SwitchA can transmit the PnP VLAN ID to SwitchB only when SwitchA meets the following conditions:

- If NETCONF is enabled on SwitchA:
  - SwitchA has registered with iMaster NCE-Campus successfully.
  - iMaster NCE-Campus has delivered a PnP VLAN ID to SwitchA, and the configuration file contains the **pnp startup-vlan** *vlan-id* command or SwitchA has negotiated a PnP VLAN ID with its upstream device.
  - iMaster NCE-Campus has delivered to SwitchA the function of transmitting the PnP VLAN ID to its downstream device, and the configuration file contains the **pnp startup-vlan send enable** command.
  - SwitchA is enabled to send LLDP packets containing PnP VLAN information to its downstream device. This function is enabled by default. If the configuration file contains the **undo lldp tlv-enable legacy-tlv pnp startup-vlan** command, the function of sending LLDP packets containing the PnP VLAN ID to the downstream device is disabled. You can enable the function on iMaster NCE-Campus.
- If NETCONF is not enabled on SwitchA:
  - SwitchA has a PnP VLAN ID configured using the **pnp startup-vlan** *vlan-id* command.
  - The **pnp startup-vlan send enable** command has been configured on SwitchA to transmit PnP VLAN information to its downstream device.
  - SwitchA is enabled to send LLDP packets containing PnP VLAN information to its downstream device. This function is enabled by default.

If the configuration file contains the **undo lldp tlv-enable legacy-tlv pnp startup-vlan** command, the function of sending LLDP packets containing the PnP VLAN ID to the downstream device is disabled. You can run the **lldp tlv-enable legacy-tlv pnp startup-vlan** command to enable this function.

SwitchB can obtain the PnP VLAN ID transmitted by SwitchA only after SwitchB is enabled to receive the PnP VLAN negotiation packets sent by its upstream device. This function is enabled by default. If the configuration file contains the **undo pnp startup-vlan receive enable** command, the function of receiving the PnP VLAN negotiation packets sent by the upstream device is disabled. You can enable the function by running **pnp startup-vlan receive enable** command.

The function of transmitting the PnP VLAN ID to the downstream device and the PnP VLAN ID can be preconfigured on controller and delivered to a switch after the switch has registered with controller. If the switch does not register with controller, perform preconfiguration on the switch.

Example

Enable the downstream device to receive the PnP VLAN negotiation packets sent by the upstream device.

```
<HUAWEI> system-view
[HUAWEI] pnp startup-vlan receive enable
```

16.15.33 pnp startup-vlan send enable

Function

The **pnp startup-vlan send enable** command enables the device to transmit the PnP VLAN ID to its downstream device.

The **undo pnp startup-vlan send enable** command disables the device from transmitting the PnP VLAN ID to its downstream device.

By default, a switch does not transmit the PnP VLAN ID to its downstream device.

Format

pnp startup-vlan send enable

undo pnp startup-vlan send enable

Parameters

None

Views

System view

Default Level

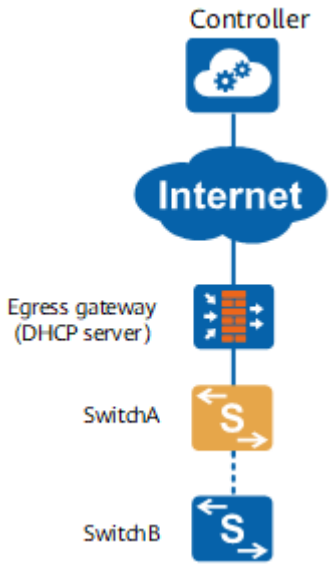
2: Configuration level

Usage Guidelines

- **Scenario 1: All switches on a CloudCampus network can be managed by iMaster NCE-Campus.**

  On the CloudCampus network shown in **Figure 16-10**, SwitchA and SwitchB are both switches. SwitchB is newly connected to the network when the VLAN for the IP address pool of the DHCP server is not VLAN 1. After SwitchB is connected to the network, by default, it uses the management VLAN 1 to send a request packet to the DHCP server to obtain the NETCONF enabling configuration, IP address, and information of iMaster NCE-Campus. However, SwitchB fails to obtain the information because the VLAN for the IP address pool of the DHCP server is not VLAN 1.

  Figure 16-10 CloudCampus networking

  To address the problem, configure PnP VLAN auto-negotiation on SwitchA. After SwitchB starts, SwitchA transmits the PnP VLAN ID to SwitchB through PnP VLAN auto-negotiation, so that SwitchB can use the PnP VLAN to obtain related information from the DHCP server.

  SwitchA can transmit the PnP VLAN ID to SwitchB only when SwitchA meets the following conditions:

  – SwitchA has registered with iMaster NCE-Campus successfully.
  – iMaster NCE-Campus has delivered a PnP VLAN ID to SwitchA, and the configuration file contains the **pnp startup-vlan** *vlan-id* command or SwitchA has negotiated a PnP VLAN ID with its upstream device.
  – iMaster NCE-Campus has delivered the function of transmitting the PnP VLAN ID to the downstream device to SwitchA, and the configuration file contains the **pnp startup-vlan send enable** command.
  – SwitchA is enabled to send LLDPDUs containing PnP VLAN information to its downstream device. This function is enabled by default. If the configuration file contains the **undo lldp tlv-enable legacy-tlv pnp startup-vlan** or **undo lldp tlv-enable legacy-tlv pnp all** command, the function of sending LLDPDUs containing the PnP VLAN ID to the

downstream device is disabled. You can enable the function on iMaster NCE-Campus.

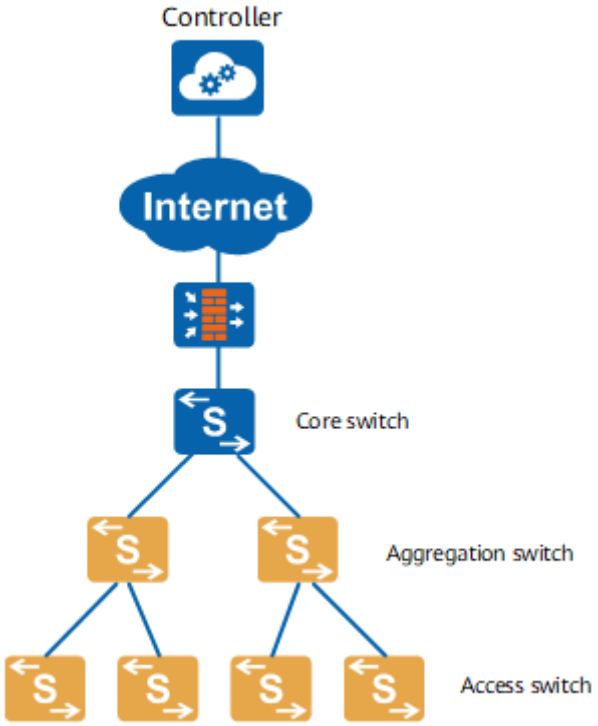
SwitchB can obtain the PnP VLAN ID transmitted by SwitchA only after SwitchB is enabled to receive the PnP VLAN negotiation packets sent by its upstream device. This function is enabled by default. If the configuration file contains the **undo pnp startup-vlan receive enable** command, the function of receiving the PnP VLAN negotiation packets sent by the upstream device is disabled. You can enable the function on iMaster NCE-Campus.

The function of transmitting the PnP VLAN ID to the downstream device and the PnP VLAN ID can be preconfigured on iMaster NCE-Campus and delivered to a switch after the switch has registered with iMaster NCE-Campus.

- **Scenario 2: On a CloudCampus network, some switches cannot be managed by iMaster NCE-Campus.**

  On the CloudCampus network shown in **Figure 16-11**, the access and aggregation switches can be managed by iMaster NCE-Campus. The core switch is not managed by iMaster NCE-Campus. When the management VLAN is changed on iMaster NCE-Campus from VLAN 1 (default) to VLAN 2, the core switch needs to notify its downstream switches of the new management VLAN ID.

  Figure 16-11 CloudCampus networking



  Configure PnP VLAN auto-negotiation on the core switch so that the core switch can notify its downstream switches of the new management VLAN ID. This process consists of the following operations:

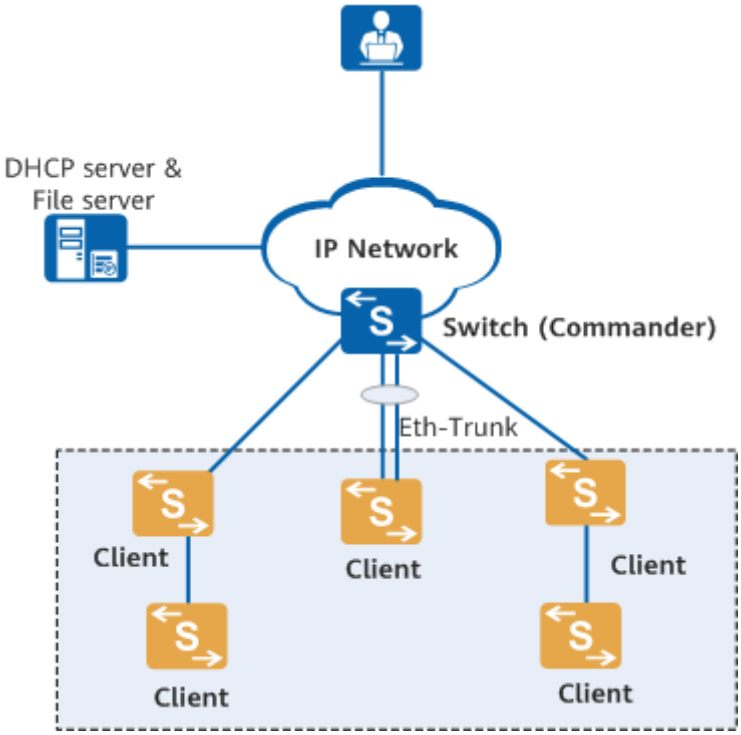
  - Run the **pnp startup-vlan** command to configure a PnP VLAN ID.
  - Run the **pnp startup-vlan send enable** command to enable the switch to transmit the PnP VLAN ID to its downstream devices.

- Run the **lldp tlv-enable legacy-tlv pnp all** command to enable the device to send LLDPDUs containing PnP information to its downstream devices. This function is enabled by default. LLDPDUs carry PnP information, including the PnP VLAN ID, Eth-Trunk enabling flag, LACP mode flag, and device type.
- If the core switch and the aggregation switches are connected through Eth-Trunks, you also need to run the **pnp startup-link-aggregation enable** command to enable the function of notifying downstream devices of the need to establish an Eth-Trunk. After the command is run, the downstream devices will automatically add interfaces to Eth-Trunks based on the negotiation. LLDPDUs carry the Eth-Trunk enabling flag and LACP mode flag.

- **Scenario 3: Zero-touch deployment using EasyDeploy**

  In **Figure 16-12**, when EasyDeploy is used for zero touch deployment, the Commander needs to notify a client of the new VLAN ID if the Commander does not use VLAN 1 to communicate with the client.

  Figure 16-12 EasyDeploy networking diagram



- Configure PnP VLAN auto-negotiation on the Commander to enable the Commander to notify clients of the new VLAN ID. This process consists of the following operations:
  - Run the **pnp startup-vlan** command to configure a PnP VLAN ID.
  - Run the **pnp startup-vlan send enable** command to enable the switch to transmit the PnP VLAN ID to its downstream devices.
  - Run the **lldp tlv-enable legacy-tlv pnp all** command to enable the device to send LLDPDUs containing PnP information to its downstream devices. This function is enabled by default. LLDPDUs carry PnP information, including the PnP VLAN ID, Eth-Trunk enabling flag, LACP mode flag, and device type.

– If the core switch and the aggregation switches are connected through Eth-Trunks, you also need to run the **pnp startup-link-aggregation enable** command to enable the function of notifying downstream devices of the need to establish an Eth-Trunk. After the command is run, the downstream devices will automatically add interfaces to Eth-Trunks based on the negotiation. LLDPDUs carry the Eth-Trunk enabling flag and LACP mode flag.

Example

Enable a switch to transmit the PnP VLAN ID to its downstream devices.

```
<HUAWEI> system-view
[HUAWEI] pnp startup-vlan send enable
```

16.15.34 redirected-controller backup ip-address

Function

The **redirected-controller backup ip-address** command configures the redirected IP address and port number of the standby iMaster NCE-Campus.

The **undo redirected-controller backup ip-address** command deletes the redirected IP address and port number of the standby iMaster NCE-Campus.

By default, no redirected IP address and port number of the standby iMaster NCE-Campus are configured on a switch.

Format

redirected-controller backup ip-address *ip-address* **port** *port-number*

undo redirected-controller backup ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies a redirected IP address.	The value is in dotted decimal notation.
port *port-number*	Specifies a redirected port number.	The value is an integer in the range 1 to 65535.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Assume that a switch has successfully registered with iMaster NCE-Campus through DHCP. After a restart, the switch will use DHCP to obtain the IP address of iMaster NCE-Campus for registration. If you want the switch to use the IP address already obtained during the previous registration, fix the IP address on iMaster NCE-Campus. Then, iMaster NCE-Campus delivers this command to the switch, and the switch executes this command to save the IP address of iMaster NCE-Campus.

Precautions

- After a restart, the switch can obtain the address of iMaster NCE-Campus using different methods (listed in descending order of priority): configured in the callhome template view on the switch, from the redirection information of iMaster NCE-Campus configured on the switch, through DHCP, using commands, or in the registration query center.
- When the following conditions are met, a switch regenerate the redirection configuration command: (1) iMaster NCE-Campus delivers redirection information to the switch to fix the IP address of iMaster NCE-Campus on the switch; (2) the **undo redirected-controller backup ip-address** command is run on the switch to delete redirection information ; (3) the configuration is saved and the switch is restarted.

Example

Configure the redirected IP address and port number of the standby iMaster NCE-Campus on a switch.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] redirected-controller backup ip-address 10.1.1.2 port 10020
```

16.15.35 redirected-controller ip-address

Function

The **redirected-controller ip-address** command configures the redirection IP address and port number of iMaster NCE-Campus.

The **undo redirected-controller ip-address** command deletes the redirection IP address and port number of iMaster NCE-Campus.

By default, no redirection IP address and port number are configured for iMaster NCE-Campus on a switch.

Format

redirected-controller ip-address *ip-address* **port** *port-number*

undo redirected-controller ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the redirection IP address.	The value is in dotted decimal notation.
port *port-number*	Specifies the redirection port number.	The value is an integer in the range 1 to 65535.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Assume that a switch has successfully registered with iMaster NCE-Campus through DHCP. After a restart, the switch will use DHCP to obtain the IP address of iMaster NCE-Campus for registration. If you want the switch to use the IP address already obtained during the previous registration, fix the IP address on iMaster NCE-Campus. Then, iMaster NCE-Campus delivers this command to the switch, and the switch executes this command to save the IP address of iMaster NCE-Campus.

Precautions

- After a restart, the switch can obtain the address of iMaster NCE-Campus using different methods (listed in descending order of priority): configured in the callhome template view on the switch, from the redirection information of iMaster NCE-Campus configured on the switch, through DHCP, using commands, or in the registration query center.
- When the following conditions are met, a switch regenerate the redirection configuration command: (1) iMaster NCE-Campus delivers redirection information to the switch to fix the IP address of iMaster NCE-Campus on the switch; (2) the **undo redirected-controller ip-address** command is run on the switch to delete redirection information ; (3) the configuration is saved and the switch is restarted.

Example

Configure the redirection IP address and port number of iMaster NCE-Campus on the switch.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] redirected-controller ip-address 10.1.1.2 port 10020
```


16.15.36 reset cloud-mng work-mode

Function

The **reset cloud-mng work-mode** command clears the cloud-based management flag in the flash memory of a switch.

Format

reset cloud-mng work-mode

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Since V200R019C00, you no longer need to change the working mode of a switch to cloud-mng to implement cloud-based management. Instead, you can enable NETCONF on the switch to implement cloud-based management. However, after a switch working in cloud-mng mode is upgraded from an earlier version to V200R019C10 or a later version, the cloud-based management flag still exists in the flash memory of the switch. As a result, the LNP, VCMP, and OPS functions do not take effect.

To resolve this problem, run the **reset cloud-mng work-mode** command to clear the cloud-based management flag in the flash memory of the switch.

- When you run the **undo netconf** command on a switch that originally worked in cloud-mng mode before the upgrade, the following message is displayed to prompt you to run the **reset cloud-mng work-mode** command to restore the LNP, VCMP, and OPS functions:
  ```
  Info: After the device is upgraded in cloud management mode, execute 'reset cloud-mng work-mode' to restore the LNP, VCMP, and OPS functions.
  ```
  When you run the **reset cloud-mng work-mode** command, the switch displays the following message indicating that this operation will delete the saved configuration and the device will restart. Exercise caution when performing this operation.
  ```
  Warning: The action will delete the saved configuration and reboot. Continue? [Y/N]:
  ```
- When you run the **reset cloud-mng work-mode** command on a switch that did not work in cloud-mng mode before the upgrade, the following message is displayed indicating that this operation is not required:
  ```
  Info: Current status is not upgrade from Cloud-mng mode.
  ```


Example

Clear the cloud-based management flag in the flash memory of a switch.

```
<HUAWEI> reset cloud-mng work-mode
```

16.15.37 reset netconf db-configuration

Function

The **reset netconf db-configuration** command clears the database configuration.

Format

reset netconf db-configuration

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To stop providing network services, run the **reset netconf db-configuration** command to clear all database configuration.

Precautions

After the **reset netconf db-configuration** or **reset saved-configuration** command is run, the **assign trunk** command configuration is cleared, that is, the default configuration is restored.

NOTICE

After the **reset netconf db-configuration** command is executed, the system asks whether you want to restart the switch. If you enter Y, the switch restarts and clears all the database and configuration file information. Confirm your action.

Example

Clear the database configuration on a switch.

```
<HUAWEI> system-view
[HUAWEI] reset netconf db-configuration
```



```
Warning: This operation will clear the database and saved configuration and restart the device. Continue?
[Y/N]:
```

16.15.38 reset netconf register-fail-record

Function

The **reset netconf register-fail-record** command clears records about failed registrations with iMaster NCE-Campus.

Format

reset netconf register-fail-record

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **reset netconf register-fail-record** command to clear records about failed registries with iMaster NCE-Campus. Confirm the action before running this command.

Example

Clear records about failed registrations with iMaster NCE-Campus.

```
<HUAWEI> reset netconf register-fail-record
Warning: This command will clear the registration failures. Continue? [Y/N]: y
```

16.15.39 { rsa | dsa } local-key-pair create (NETCONF view)

Function

The **{ rsa | dsa } local-key-pair create** command creates a local RSA or DSA key pair.

Format

{ rsa | dsa } local-key-pair create

Parameters

Parameter	Description	Value
rsa	Creates a local RSA key pair.	-
dsa	Creates a local DSA key pair.	-

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

You can run this command to create a local RSA or DSA key pair. If the local RSA or DSA key pair already exists, the system displays a message asking you whether to create a new one.

Example

Create a local DSA key pair.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] dsa local-key-pair create
```

16.15.40 set netconf db-configuration-file

Function

The **set netconf db-configuration-file** command configures a NETCONF database file used by the system.

NOTE

This command is supported only in scenarios where the device is registered with iMaster NCE-Campus.

Format

set netconf db-configuration-file *database-file*

Parameters

Parameter	Description	Value
database-file	Specifies a database file. The file must already exist. **NOTE** You must specify a database file in the **flash:/** directory on the active device.	The value is a string of 5 to 64 characters in the format of [*drive-name*] [*file-name*]. It cannot contain spaces. • If *drive-name* is not specified, the default flash memory name is used. • The value of *file-name* cannot contain special characters including | ; & $ < > ' ! \ and must use .rdb as the file name extension.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the database file is abnormal due to misoperations or system exceptions, you can run the **set netconf db-configuration-file** command to manually specify a valid database file. To view the currently effective database file, run the **display netconf configuration** command.

NOTICE

When you run this command, the system displays a message indicating that the device will be disconnected from iMaster NCE-Campus for a short period of time. After you enter **Y**, the device is disconnected for a short period of time and then reconnects to iMaster NCE-Campus. Therefore, exercise caution when running this command.

Prerequisites

The configurations in the database file must be the same as those in the configuration file. Therefore, before running this command, configure the

corresponding configuration file and make it take effect by using one of the following methods:

- Run the **startup saved-configuration** command to configure the configuration file used by the system, and then restart the system for the configuration file to take effect. You are advised to use the backup configuration file in the backup directory.
- Manually supplement configurations in the configuration file and make the configurations take effect.

Precautions

- When you run this command to configure a database file, the system checks the file content. If the file content is invalid, the command configuration fails and the configurations in the configuration file may be lost. To ensure validity of the database file, you are advised to use the backup database file.
- The database file specified in this command cannot exceed 30 MB or be named **startup.rdb**. Otherwise, the configuration fails.
- This command cannot be executed repeatedly in a short period of time.

Example

Specify **2022-06-23_startup.rdb** as the system datastore file.

```
<HUAWEI> set netconf db-configuration-file configbackup/2022-06-23_startup.rdb
Warning: Configure the corresponding CFG file first. This operation will activate the database configuration
file and make the device go offline for a short period of time, Continue? [Y/
N]:y
Info: The operation is in progress. Please wait.....Done.
```

16.15.41 source ip

Function

The **source ip** command configures the IPv4 address and port number used by a switch to communicate with the NMS through NETCONF.

The **undo source ip** command deletes the IPv4 address and port number used by a switch to communicate with the NMS through NETCONF.

By default, no IPv4 address and port number are configured for a switch to communicate with the NMS through NETCONF.

Format

source ip { *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* } [**port** *port-number*]

undo source ip

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of a switch.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance to which the IPv4 address or interface of the switch belongs.	The value must be an existing VPN instance name.
interface *interface-type interface-number*	Specifies the interface to which the IPv4 address used by the switch belongs.	The interface must be an existing Layer 3 interface on the switch. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.
port *port-number*	• This parameter is the port number used by the switch in NETCONF over SSH Callhome mode. • This parameter is the port number used by both the switch and NMS in NETCONF over SSH mode.	The value is 830 or an integer in the range 55552 to 55807. The default value is 830.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS needs to configure and manage a switch using NETCONF, run the **source ip** command to configure the IPv4 address and port number used by the switch to communicate with the NMS, regardless of whether the NETCONF over SSH or NETCONF over SSH Callhome mode is used.

Precautions

- You cannot run this command if you have run the **source ip-address** command in the SMI view to configure the IPv4 address used by the switch to communicate with an NMS (for example, iMaster NCE-CampusInsight).

- When you run the **source ip** command to configure or change the port number for IPv4 communication between the switch and NMS, the port number for IPv6 communication between the two systems configured using the **source ipv6-address** command will be changed accordingly.
- Changing the IPv4 address or port number will cause communication interruption between the switch and NMS.

Example

Set the IPv4 address and port number used by the switch to communicate with the NMS through NETCONF to 10.1.1.1 and 55555, respectively.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] source ip 10.1.1.1 port 55555
```

16.15.42 source ipv6-address

Function

The **source ipv6-address** command configures the IPv6 address and port number used by a switch to communicate with the NMS through NETCONF.

The **undo source ipv6-address** command deletes the IPv6 address and port number used by a switch to communicate with the NMS through NETCONF.

By default, no IPv6 address and port number are configured for a switch to communicate with the NMS using NETCONF.

Format

source ipv6-address { *ipv6-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* } [**port** *port-number*]

undo source ipv6-address

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a switch.	The total length of the value is 128 bits, which are divided into eight groups. Each group contains four hexadecimal digits. The value is in the format of X:X:X:X:X:X:X:X.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance to which the IPv6 address or interface of the switch belongs.	The value must be an existing VPN instance name.

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface to which the IPv6 address used by the switch belongs.	The interface must be an existing Layer 3 interface on the switch. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.
port *port-number*	Specifies the port number used by the switch and NMS.	The value is 830 or an integer in the range 55552 to 55807. The default value is 830.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS needs to configure and manage a switch using an IPv6 address in NETCONF over SSH mode, run the **source ipv6-address** command to configure the IPv6 address and port number of the switch.

Precautions

When you run the **source ipv6-address** command to configure or change the port number for IPv6 communication between the switch and NMS, the port number for IPv4 communication between the two systems configured using the **source ip** command will be changed accordingly.

Changing the IPv6 address or port number will cause communication interruption between the switch and NMS.

Example

Set the IPv6 address and port number used by the switch to communicate with the NMS through NETCONF to FC00::1 and 55555, respectively.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] source ipv6-address FC00::1 port 55555
```


16.15.43 user assign { rsa | dsa } public-key

Function

The **user** *user-name* **assign { rsa | dsa } public-key public-key-name** command assigns an existing RSA or DSA public key to a specified user.

The **undo user** *user-name* **assign { rsa | dsa } public-key** command deletes the mapping between a user and an RSA or DSA public key.

By default, no RSA or DSA public key is assigned to a user.

Format

user *user-name* **assign { rsa | dsa } public-key** *public-key-name*

undo user *user-name* **assign { rsa | dsa } public-key**

Parameters

Parameter	Description	Value
user-name	Specifies a NETCONF user name.	The value is a string of 1 to 25 case-insensitive characters without spaces. **NOTE** If the string is enclosed in quotation marks, the string can contain spaces.
rsa	Assigns an RSA public key to a specified user.	-
dsa	Assigns a DSA public key to a specified user.	-
public-key-name	Specifies the name of an RSA or DSA public key.	The value is a string of 1 to 30 case-insensitive characters without spaces. **NOTE** If the string is enclosed in double quotation marks ("), the string can contain spaces.

Views

NETCONF view

Default Level

3: Management level

Usage Guidelines

When a controller acting as a NETCONF client needs to log in to the switch acting as the NETCONF server in RSA or DSA mode, you can run this command to assign an RSA or DSA public key to a specified user. If multiple public keys are assigned to a user, the last assigned public key takes effect.

Example

Assign the DSA public key **key1** to the NETCONF user named **test123**.

```
<HUAWEI> system-view
[HUAWEI] netconf
[HUAWEI-netconf] user test123 assign dsa public-key key1
```

16.16 O&M information reporting Configuration Commands

16.16.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.16.2 collect dynamic mac disable

Function

The **collect dynamic mac disable** command disables the device from reporting dynamic MAC address information to an NMS.

The **undo collect dynamic mac disable** command enables the device to report dynamic MAC address information to an NMS.

By default, the function of reporting dynamic MAC address information to an NMS is enabled in the system view, but not the interface view.

Format

collect dynamic mac disable

undo collect dynamic mac disable

Parameters

None

Views

System view, Ethernet interface view, GE interface view, XGE interface view, Multi-GE interface view, 25GE interface view, 40GE interface view, 100GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After being connected to an NMS (for example, a controller or analyzer), the device also reports information about online users who go online after successful authentication or without authentication to NMS. The information about users who go online without authentication includes dynamic MAC addresses learned by the device. Layer 2 network devices usually learn a large number of dynamic MAC addresses, which will be sent to the NMS if the **collect-item user-data enable** command is configured. As a result, large amounts of resources on the NMS will be occupied. To reduce the usage of NMS resources, you can run the **collect dynamic mac disable** command to disable the device from reporting dynamic MAC address information to the NMS.

Precautions

- The device reports dynamic MAC address information to an NMS only when the **undo collect dynamic mac disable** command is run in both the system view and interface view.
- This command does not take effect on the device's interface connected to the NMS.
- In a policy association scenario, ASs cannot report dynamic MAC address information to the NMS.

Example

Disable all interfaces on the device from reporting dynamic MAC address information to the NMS.

```
<HUAWEI> system-view
[HUAWEI] collect dynamic mac disable
```

16.16.3 collect-item enable (SMI view)

Function

The **collect-item enable** command enables the switch to report collected information to iMaster NCE-CampusInsight.

The **undo collect-item enable** command disables the switch from reporting collected information to iMaster NCE-CampusInsight.

By default, the switch does not report any collected information to iMaster NCE-CampusInsight.

Format

collect-item { **device-data** | **fiber-module** | **poe** | **user-data** | **device-status** | **media-quality** | **application-statistics-data** | **sipfpm-data** } **enable**

undo collect-item { **device-data** | **fiber-module** | **poe** | **user-data** | **device-status** | **media-quality** | **application-statistics-data** | **sipfpm-data** } **enable**

Parameters

Parameter	Description	Value
device-data	Enables the switch to report device data to iMaster NCE-CampusInsight.	-
fiber-module	Enables the switch to report optical module information to iMaster NCE-CampusInsight.	-
poe	Enables the switch to report PoE data to iMaster NCE-CampusInsight.	-
user-data	Enables the switch to report traffic statistics collection of wired users to iMaster NCE-CampusInsight.	-
device-status	Enables the switch to report device status information to iMaster NCE-CampusInsight.	-
media-quality	Enables the switch to report application-based poor-QoE monitoring information, audio, and video data to iMaster NCE-CampusInsight.	-
application-statistics-data	Enables the switch to report application traffic statistics to iMaster NCE-CampusInsight.	Only the following models support this parameter: S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, S6730S-S
sipfpm-data	Enables the switch to report packet loss and delay measurement information to iMaster NCE-CampusInsight.	-

Views

SMI view

Default Level

3: Management level

Usage Guidelines

Based on your networking requirements, you can enable the switch to report collected information to iMaster NCE-CampusInsight. You can run this command for multiple times to enable the switch to report different types of data to iMaster NCE-CampusInsight. For details about the information that can be collected, see KPI.

Example

Enable the switch to report optical module information to iMaster NCE-CampusInsight.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] collect-item fiber-module enable
```

16.16.4 collect-item interval (SMI view)

Function

The **collect-item interval** command sets the interval at which the switch collects KPI information.

The **undo collect-item interval** command restores the default interval at which the switch collects KPI information.

By default, the interval for collecting KPI information about the total number of bad blocks in the NAND flash and the total number of erase times in the NOR flash is 60 minutes, and the interval for collecting other KPI information is 5 minutes.

Format

collect-item { **device-data** | **fiber-module** | **poe** | **user-data** | **device-status** } **interval** *interval*

undo collect-item { **device-data** | **fiber-module** | **poe** | **user-data** | **device-status** } **interval**

Parameters

Parameter	Description	Value
device-data	Enables the switch to report device data to iMaster NCE-CampusInsight.	-
fiber-module	Enables the switch to report optical module information to iMaster NCE-CampusInsight.	-

Parameter	Description	Value
poe	Enables the switch to report PoE data to iMaster NCE-CampusInsight.	-
user-data	Enables the switch to report traffic statistics collection of wired users to iMaster NCE-CampusInsight.	-
device-status	Enables the switch to report device status information to iMaster NCE-CampusInsight.	-
interval *interval*	Specifies the interval at which the switch collects KPI information.	The value is an integer in the range from 1 to 1440, in minutes.

Views

SMI view

Default Level

3: Management level

Usage Guidelines

Based on your networking requirements, you can set the interval at which the switch collects KPI information. For details about the information that can be collected, see KPI.

Example

Enable the switch to report optical module information to the iMaster NCE-CampusInsightand set the interval at which the switch collects such information to 3 minutes.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] collect-item fiber-module enable
[HUAWEI-smi-server] collect-item fiber-module interval 3
```

16.16.5 collect-item syslog enable (SMI view)

Function

The **collect-item syslog enable** command configures the device to report logs and alarms to an NMS.

The **undo collect-item syslog enable** command disables the device from reporting logs and alarms to an NMS.

By default, the device does not report logs and alarms to an NMS.

Format

collect-item syslog { **aaa** | **acl** | **am** | **arp** | **basetrap** | **bgp** | **defd** | **dhcp** | **dldp** | **dot1x** | **efm** | **emdi** | **entitytrap** | **errdown** | **gtl** | **ifnet** | **ifpdt** | **ipca** | **l2ifppi** | **l3adp** | **lbdt** | **mcast** | **mpls** | **mstp** | **nac** | **nvo3** | **ospf** | **poe** | **portal** | **rumng** | **ruupgrade** | **sea** | **sece** | **shell** | **srm** | **web** | **gtl** | **qose** | **entityexttrap** | **fsp** | **mad** } **enable**

undo collect-item syslog { **aaa** | **acl** | **am** | **arp** | **basetrap** | **bgp** | **defd** | **dhcp** | **dldp** | **dot1x** | **efm** | **emdi** | **entitytrap** | **errdown** | **gtl** | **ifnet** | **ifpdt** | **ipca** | **l2ifppi** | **l3adp** | **lbdt** | **mcast** | **mpls** | **mstp** | **nac** | **nvo3** | **ospf** | **poe** | **portal** | **rumng** | **ruupgrade** | **sea** | **sece** | **shell** | **srm** | **web** | **am** | **qose** | **entityexttrap** | **fsp** | **mad** } **enable**

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S can report data of the eMDI and iPCA modules to an NMS.

Parameters

Parameter	Description	Value
aaa	Configures the device to report data of the AAA module to an NMS.	-
acl	Configures the device to report data of the ACL module to an NMS.	-
am	Configures the device to report data of the AM module to an NMS.	-
basetrap	Configures the device to report data of the BASETRAP module to an NMS.	-
bgp	Configures the device to report data of the BGP module to an NMS.	-
defd	Configures the device to report data of the DEFD module to an NMS.	-
dhcp	Configures the device to report data of the DHCP module to an NMS.	-
dldp	Configures the device to report data of the DLDP module to an NMS.	-
dot1x	Configures the device to report data of the DOT1X module to an NMS.	-

Parameter	Description	Value
efm	Configures the device to report data of the EFM module to an NMS.	-
emdi	Configures the device to report data of the eMDI module to an NMS.	-
entitytrap	Configures the device to report data of the ENTITYTRAP module to an NMS.	-
errdown	Configures the device to report data of the ErrorDown module to an NMS.	-
gtl	Configures the device to report data of the GTL module to an NMS.	-
ifnet	Configures the device to report data of the IFNET module to an NMS.	-
ifpdt	Configures the device to report data of the IFPDT module to an NMS.	-
ipca	Configures the device to report data of the iPCA module to an NMS.	-
l2ifppi	Configures the device to report data of the L2IFPPI module to an NMS.	-
l3adp	Configures the device to report data of the L3MB module to an NMS.	-
lbdt	Configures the device to report data of the LBDT module to an NMS.	-
mcast	Configures the device to report data of the MCAST module to an NMS.	-
mpls	Configures the device to report data of the MPLS module to an NMS.	-
mstp	Configures the device to report data of the MSTP module to an NMS.	-
nac	Configures the device to report data of the NAC module to an NMS.	-

Parameter	Description	Value
nvo3	Configures the device to report data of the NVO3 module to an NMS.	-
ospf	Configures the device to report data of the OSPF module to an NMS.	-
poe	Configures the device to report data of the PoE module to an NMS.	-
portal	Configures the device to report data of the Portal module to an NMS.	-
qose	Configures the device to report data of the QoS module to an NMS.	-
rumng	Configures the device to report data of the RUMNG module to an NMS.	-
ruupgrade	Configures the device to report data of the RUUPGRADE module to an NMS.	-
sea	Configures the device to report data of the SEA module to an NMS.	-
sece	Configures the device to report data of the SECE module to an NMS.	-
shell	Configures the device to report data of the SHELL module to an NMS.	-
srm	Configures the device to report data of the SRM module to an NMS.	-
web	Configures the device to report data of the WEB module to an NMS.	-
entityexttrap	Configures the device to report data of the ENTITYEXTTRAP module to an NMS.	-
arp	Configures the device to report data of the ARP module to an NMS.	-
fsp	Configures the device to report data of the FSP module to an NMS.	-

Parameter	Description	Value
mad	Configures the device to report data of the MAD module to an NMS.	-

Views

SMI view

Default Level

3: Management level

Usage Guidelines

You can run this command to configure the device to report logs and alarms to an NMS. You can run the command multiple times to configure the device to report multiple types of data to the NMS. For the device information that can be collected, see Logs and Alarms.

Example

Configure the device to report data of the ACL module to an NMS.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] collect-item syslog acl enable
```

16.16.6 keepalive (SMI view)

Function

The **keepalive** command configures connection parameters between the switch and iMaster NCE-CampusInsight.

The **undo keepalive** command restores the default settings of connection parameters between the switch and iMaster NCE-CampusInsight.

By default, the switch and iMaster NCE-CampusInsight send heartbeat packets to each other at an interval of 5 minutes, the switch reconnects to iMaster NCE-CampusInsight at an interval of 5 minutes, and the maximum number of reconnection attempts is 0.

Format

keepalive { **interval** *interval* | **retry-interval** *retry-interval* | **retry-number** *retry-number* } *

undo keepalive { **interval** | **retry-interval** | **retry-number** } *

Parameters

Parameter	Description	Value
interval *interval*	Sets the interval at which the switch and iMaster NCE-CampusInsight send heartbeat packets to each other.	The value is an integer in the range from 5 to 60, in minutes.
retry-interval *retry-interval*	Sets the interval at which the switch reconnects to iMaster NCE-CampusInsight after port disconnection for the first time.	The value is an integer in the range from 5 to 60, in minutes.
retry-number *retry-number*	Sets the maximum number of attempts the switch reconnects to iMaster NCE-CampusInsight after port disconnection for the first time.	The value is an integer in the range from 0 to 10. The default value is 0, which indicates that the switch attempts to reconnect to iMaster NCE-CampusInsight until the reconnection succeeds.

Views

SMI view

Default Level

3: Management level

Usage Guidelines

According to the network stability, you can adjust connection parameters between the switch and iMaster NCE-CampusInsight as required, such as the interval at which the switch and iMaster NCE-CampusInsight send heartbeat packets to each other and the maximum number of reconnection attempts. If the network condition is poor, set the maximum number of reconnection attempts to a smaller value and the reconnection interval to a large value to consume less network resources.

Example

Set the interval at which the switch reconnects to iMaster NCE-CampusInsight to 10 minutes and the maximum number of reconnection attempts to 5.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] keepalive retry-interval 10 retry-number 5
```


16.16.7 max-packet-size (SMI view)

Function

The **max-packet-size** command sets the maximum size of packets sent by the switch to report KPI information to iMaster NCE-CampusInsight.

The **undo max-packet-size** command restores the default maximum size of packets sent by the switch to report KPI information to iMaster NCE-CampusInsight.

By default, the maximum size of packets sent by the switch to report KPI information to iMaster NCE-CampusInsight is 5 KB.

Format

max-packet-size *size*

undo max-packet-size

Parameters

Parameter	Description	Value
size	Specifies the maximum packet size.	The value is an integer in the range from 5 to 15, in KB.

Views

SMI view

Default Level

3: Management level

Usage Guidelines

According to the network condition, you can run this command to set the maximum size of packets sent by the switch to report KPI information to iMaster NCE-CampusInsight. If the network condition is poor, set the maximum size of packets sent by the switch to report KPI information to iMaster NCE-CampusInsight to a smaller value to reduce packet loss.

Example

Set the maximum size of packets sent by the switch to report KPI information to iMaster NCE-CampusInsight to 10 KB.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] max-packet-size 10
```


16.16.8 monitor application name

Function

The **monitor application name** command enables application-based poor-QoE monitoring for a specified application.

The **undo monitor application name** command disables application-based poor-QoE monitoring.

By default, application-based poor-QoE monitoring is disabled for an application.

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

monitor application name *appname*

undo monitor application name *appname*

Parameters

Parameter	Description	Value
appname	Specifies the name of an application.	The value is a string of characters. The value depends on the applications supported in the signature database. To check the supported application names, run the **display application** command.

Views

SEA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor the quality of applications, you can configure the application-based poor-QoE monitoring function. After this function is configured, the device reports the application quality at a specific statistical interval. Application-based poor-QoE monitoring information reporting supports applications that use TCP or UDP-RTP as well as user-defined applications. Poor-QoE monitoring information can be reported for the following applications that use UDP-RTP: Skype_VoIP (Skype multimedia chat), Fetion_VoIP (Fetion multimedia chat), RTP, WhatsAPP, eSpace_VoIP (eSpace multimedia chat), WeLink_VideoCall (WeLink video call), Microsoft Teams, WebEx_VoIP (WebEx multimedia chat), and Hangouts.

Prerequisites

The eMDI detection function has been enabled using the **emdi** command.

Precautions

When poor-QoE monitoring based on users and applications has been configured using the **monitor source ucl-group** command, you cannot run the **monitor application name** command to configure application-based poor-QoE monitoring.

Example

Enable application-based poor-QoE monitoring for the application named **RTP**.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] quit
[HUAWEI] sea
[HUAWEI-sea] monitor application name RTP
```

16.16.9 monitor application period

Function

The **monitor application period** command configures an application-based poor-QoE monitoring interval.

The **undo monitor application period** command restores the default application-based poor-QoE monitoring interval.

By default, the application-based poor-QoE monitoring interval is 10 seconds.

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

monitor application period *period-value*

undo monitor application period

Parameters

Parameter	Description	Value
period-value	Specifies the maximum packet size.	The value is of the enumerated type, and can only be 2, 5, 10, 30, and 60, in seconds.

Views

SEA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to configure the application-based poor-QoE monitoring interval based on your network conditions. To obtain the application quality in a timely manner, you can configure a small monitoring interval.

Prerequisites

The eMDI detection function has been enabled using the **emdi** command.

Example

Set the application-based poor-QoE monitoring interval to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] quit
[HUAWEI] sea
[HUAWEI-sea] monitor application period 30
```

16.16.10 monitor source ucl-group

Function

The **monitor source ucl-group** command is used to configure poor-QoE monitoring based on users or users and applications.

The **undo monitor source ucl-group** command deletes the configuration of poor-QoE monitoring based on users or users and applications.

By default, poor-QoE monitoring based on users or users and applications is not configured.

NOTE

Only the S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this command.

Format

monitor source ucl-group { *group-index* | **name** *group-name* } [**application name** *appname*]

undo monitor source ucl-group { *group-index* | **name** *group-name* } [**application name** *appname*]

Parameters

Parameter	Description	Value
group-index	Specifies the index of a UCL group.	The value is an integer in the range from 1 to 64000.
name *group-name*	Specifies the name of a UCL group.	The UCL group must exist.
application name *appname*	Specifies the name of an application.	The value is a string of characters. The value depends on the applications supported in the signature database. To check the supported application names, run the **display application** command. A maximum of 16 application names can be configured at a time.

Views

SEA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the intelligent O&M solution, the administrator wants to obtain information about the network quality experienced by users. A campus network has a large number of access users. During user access authentication, users with the same network access rights are added to the same UCL group. In this way, user-based network quality monitoring can be implemented based on the UCL group.

After you run this command to configure poor-QoE monitoring based on UCL groups or UCL groups and applications, the device periodically reports quality information about users or users and applications to the NMS.

Pre-configuration Tasks

The **emdi** command has been run to enable the eMDI function.

Precautions

- Poor-QoE monitoring can be performed for a maximum of 128 UCL groups.
- After you run the **monitor application name** command to perform poor-QoE monitoring on an application, you cannot run this command to perform poor-QoE monitoring based on users and applications.

Example

Configure poor-QoE monitoring for users in UCL group 10.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] quit
[HUAWEI] sea
[HUAWEI-sea] monitor source ucl-group 10
```

16.16.11 report-interval (SMI view)

Function

The **report-interval** command sets the interval at which the switch reports KPI information to iMaster NCE-CampusInsight.

The **undo report-interval** command restores the default interval at which the switch reports KPI information to iMaster NCE-CampusInsight.

By default, the switch reports KPI information to iMaster NCE-CampusInsight at an interval of 1 minute.

Format

report-interval *interval*

undo report-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which the switch reports KPI information to iMaster NCE-CampusInsight.	The value is an integer in the range from 1 to 5, in minutes.

Views

SMI view

Default Level

3: Management level

Usage Guidelines

According to the actual device and network resource usage and iMaster NCE-CampusInsight's requirements for the information collection precision, you can run this command to set the interval at which the switch reports KPI information to iMaster NCE-CampusInsight. A shorter interval indicates that KPI information is reported more frequently, the information collection precision is higher, and more device and network resources are occupied. A longer interval signifies that less information is collected by the switch within the same time period, the

information collection precision is lower, but less device and network resources are occupied.

Example

Set the interval at which the switch reports KPI information to iMaster NCE-CampusInsight to 5 minutes.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] report-interval 5
```

16.16.12 rtp-media monitor-period

Function

The **rtp-media monitor-period** command sets the monitoring period of media streams.

The **undo rtp-media monitor-period** command restores the default monitoring period of media streams.

By default, the monitoring period of media streams is 10 seconds.

Format

rtp-media monitor-period *period-value*

undo rtp-media monitor-period [*period-value*]

Parameters

Parameter	Description	Value
period-value	Specifies the monitoring period of media streams.	The value is of the enumerated type, and can only be 10, 30, and 60, in seconds.

Views

SEA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor service quality of voice and video applications transported over RTP, run the **sea** command to enable the SEA function to detect SIP sessions, and use the eMDI function to detect dynamic indicators of RTP streams. To adjust the

monitoring period of media streams, run the **rtp-media monitor-period** command.

Prerequisites

The eMDI detection function has been enabled using the **emdi** command.

Example

Set the monitoring period of media streams to 30 seconds.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] quit
[HUAWEI] sea
[HUAWEI-sea] rtp-media monitor-period 30
```

16.16.13 rtp-media monitor-type

Function

The **rtp-media monitor-type** command sets the type of media streams to be monitored.

The **undo rtp-media monitor-type** command deletes the type of media streams to be monitored.

By default, the type of media streams to be monitored is not configured.

Format

rtp-media monitor-type { **audio** | **video** } *

undo rtp-media monitor-type { **audio** | **video** } *

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support **video**.

Parameters

Parameter	Description	Value
audio	Sets the type of media streams to be monitored to audio.	-
video	Sets the type of media streams to be monitored to video.	-

Views

SEA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor service quality of audio and video applications transported over RTP in real time, you must run the **rtp-media monitor-type** command to set the type of media streams to be monitored after enabling the SEA function using the **sea** command.

Prerequisites

The eMDI detection function has been enabled using the **emdi** command.

Precautions

O&M information reporting for audio and video services takes effect only for unencrypted SIP packets without any tunnel header in IPv4 scenarios.

Example

Set the type of media streams to be monitored to audio.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] quit
[HUAWEI] sea
[HUAWEI-sea] rtp-media monitor-type audio
```

16.16.14 sea

Function

The **sea** command enables the service experience analysis (SEA) function for users and applications and displays the SEA view.

The **undo sea** command disables the SEA function and deletes the SEA view.

By default, the SEA function is disabled.

Format

sea

undo sea

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor the quality of applications (such as audio and video applications) in real time during intelligent O&M of campus networks, run the **sea** command to enable the SEA function.

Prerequisites

The eMDI detection function has been enabled using the **emdi** command.

Follow-up Procedure

Run the **rtp-media monitor-type** { **audio** | **video** } * command to configure the type of media streams to be monitored or run the **monitor application name** *appname* command enables application-based poor-QoE monitoring for a specified application.

Example

Enable the SEA function and display the SEA view.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] quit
[HUAWEI] sea
[HUAWEI-sea]
```

16.16.15 server backup ip-address (SMI view)

Function

The **server backup ip-address** command configures the IPv4 address and port number of the standby analyzer connected to a switch.

The **undo server backup ip-address** command deletes the IPv4 address and port number of the standby analyzer connected to the switch.

By default, no standby analyzer's IPv4 address and port number are configured.

Format

server backup ip-address *ip-address* [**port** *port-number*]

undo server backup ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of the standby analyzer.	The value is in dotted decimal notation.

Parameter	Description	Value
port *port-number*	Specifies the port number of the standby analyzer.	The value is an integer in the range from 0 to 65535. The default value is 0.

Views

SMI view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you configure analyzers connected to a switch for intelligent O&M, you can run the **server backup ip-address** command to configure the IPv4 address and port number of the standby analyzer. When the active analyzer breaks down or is disconnected, services can be automatically switched to the standby analyzer, ensuring service continuity.

Prerequisites

The IPv4 address of the active analyzer connected to the switch has been configured using the **server ip-address** command.

Precautions

There is no limitation on the sequence in which you delete the active and standby analyzer configurations.

Example

Configure the IPv4 address and port number of the standby analyzer.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] server ip-address 1.1.1.1 port 111
[HUAWEI-smi-server] server backup ip-address 2.2.2.2 port 222
```

16.16.16 server ip-address (SMI view)

Function

The **server ip-address** command configures the IPv4 address and port number of connected iMaster NCE-CampusInsight.

The **undo server ip-address** command deletes the IPv4 address and port number of connected iMaster NCE-CampusInsight.

By default, the IPv4 address and port number of connected iMaster NCE-CampusInsight are not configured on the switch.

Format

server ip-address *ip-address* [**port** *port-number*]

undo server ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of iMaster NCE-CampusInsight.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of iMaster NCE-CampusInsight.	The value is an integer in the range from 0 to 65535. The default value is 0.

Views

SMI view

Default Level

3: Management level

Usage Guidelines

To implement intelligent O&M, the switch needs to establish a NETCONF connection with iMaster NCE-CampusInsight and periodically reports KPI information to iMaster NCE-CampusInsight. To enable interoperability between the switch and iMaster NCE-CampusInsight, run the **server ip-address** command on the switch to configure the IPv4 address and port number of iMaster NCE-CampusInsight.

Example

Set the IP address and port number of iMaster NCE-CampusInsight to 10.1.2.1 and 27371, respectively.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] server ip-address 10.1.2.1 port 27371
```

16.16.17 smi-server

Function

The **smi-server** command creates and displays the switch maintenance insight (SMI) view.

The **undo smi-server** command deletes the SMI view.

By default, no SMI view is created on a switch.

Format

smi-server

undo smi-server

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The switch needs to interconnect with iMaster NCE-CampusInsight to implement O&M information reporting. You can run the **smi-server** command to enter the SMI view, and configure the IP address and port number used by connected iMaster NCE-CampusInsight in the SMI view.

Follow-up Procedure

Run the **server ip-address (SMI view)** command to configure the IPv4 address and port number of iMaster NCE-CampusInsight.

Precautions

Deleting the SMI view using the **undo smi-server** command will delete all O&M information reporting configurations from the switch. Therefore, exercise caution when deleting the SMI view.

Example

Create and display the SMI view.

```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server]
```

16.16.18 source ip-address (SMI View)

Function

The **source ip-address** command configures the IPv4 address used by the switch to communicate with an NMS.

The **undo source ip-address** command deletes the configuration of the IPv4 address used by the switch to communicate with an NMS.

By default, no IPv4 address is configured for the switch to communicate with an NMS.

Format

source ip-address *ip-address* [**vpn-instance** *vpn-instance-name*]

undo source ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of a switch.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be the name of an existing VPN instance.

Views

SMI view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you want an NMS (for example, iMaster NCE-CampusInsight) to monitor and analyze KPIs or traffic statistics of a switch, you must run this command to configure the IPv4 address used by the switch to communicate with the NMS.

Precautions

- When the **source ip** or **management-vlan** command is run in the NETCONF view, the switch connects to iMaster NCE-Campus in joint deployment mode. For configuration consistency purposes, you cannot run this command to configure the IP address used by the switch to communicate with iMaster NCE-CampusInsight.
- Changing the IPv4 address will interrupt the communication between the switch and NMS.

Example

Set the IPv4 address used by the switch to communicate with an NMS to 10.1.1.1.


```
<HUAWEI> system-view
[HUAWEI] smi-server
[HUAWEI-smi-server] source ip-address 10.1.1.1
```

16.17 eMDI Configuration Commands

16.17.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

16.17.2 display emdi

Function

The **display emdi** command displays the eMDI specifications, current eMDI configuration, and running status of eMDI instances.

Format

display emdi

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the eMDI specifications, current eMDI configuration, and running status of eMDI instances.

```
<HUAWEI> display emdi

Specification Information(Main Board):
 Max Instance Number                : 16
 Max UDP Instance Number            : 16
 Max TCP Instance Number            : 8
 Max Static Instance Number         : 16
 Max Dynamic Instance Number        : 16
```



```
Configuration Information:
 Current Instance Number               : 0
 Current Running Instance Number       : 0
 Current UDP Instance Number           : 0
 Current TCP Instance Number           : 0
 Current Static Instance Number        : 0
 Current Dynamic Instance Number       : 0

Specification and Configuration Information(IO Board
0):
 Max Instance Number                   : 16
 Current Instance Number               : 0
```

Table 16-93 Description of the **display emdi** command output

Item	Description
Specification Information(Main Board)	Specifications of the switch.
Max Instance Number	Maximum number of eMDI instances supported by the switch.
Max UDP Instance Number	Maximum number of eMDI instances for monitoring UDP packets.
Max TCP Instance Number	Maximum number of eMDI instances for monitoring TCP packets.
Max Static Instance Number	Maximum number of eMDI instances that can be statically configured.
Max Dynamic Instance Number	Maximum number of eMDI instances that can be dynamically configured.
Configuration Information	Configuration on the switch.
Current Instance Number	Number of eMDI instances configured on the switch.
Current Running Instance Number	Number of eMDI instances that have been started.
Current UDP Instance Number	Number of eMDI instances that are monitoring UDP packets.
Current TCP Instance Number	Number of eMDI instances that are monitoring TCP packets.
Current Static Instance Number	Number of eMDI instances that have been statically configured.
Current Dynamic Instance Number	Number of eMDI instances that have been dynamically configured.
Specification and Configuration Information(IO Board 0)	Device specifications and configuration information.

16.17.3 display emdi statistics instance

Function

The **display emdi statistics instance** command displays statistics about an eMDI instance.

Format

display emdi statistics instance *instance-id* [**verbose** | **abnormal**]

Parameters

Parameter	Description	Value
instance-id	Specifies the ID of an eMDI instance.	The value is an integer that ranges from 1 to 5120 for S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, and from 1 to 4112 for other models.
verbose	Displays detailed statistics about an eMDI instance.	-
abnormal	Displays exception statistics collected by an eMDI instance. • For service traffic transmitted over UDP, an exception occurs if the value of **RTP-LR** field in the command output is not 0. • For service traffic transmitted over TCP, an exception occurs if the value of **UPLR** or **DPLR** in the command output is not 0.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays only the latest 60 statistical records of an eMDI instance.

Example

Display statistics about eMDI instance 1 that monitors UDP flows.

```
<HUAWEI> display emdi statistics instance 1
Instance ID : 1       Monitor Period(s) : 10    Protocol : UDP
------------------------------------------------------------------------------
      Record        Monitor       RTP-LR       RTP-SER       Jitter
       Time         Status     (1/100000)    (1/100000)      (us)
2018-09-17:16-17-00  Normal         152           151           2
2018-09-17:16-17-10  Normal         152           151           2
2018-09-17:16-17-20  Normal         152           151           2
```

Display statistics about eMDI instance 2 that monitors TCP flows.

```
<HUAWEI> display emdi statistics instance 2
Instance ID : 2       Monitor Period(s) : 10    Protocol : TCP
------------------------------------------------------------------------------
      Record        Monitor       MFR          DPLR         UPLR      DRTT
      Time          Status       (bps)      (1/100000)   (1/100000)   (us)
------------------------------------------------------------------------------
2018-09-17:16-17-00  Normal      4865656118    151          2         2
2018-09-17:16-17-10  Normal      4866005390    151          2         2
2018-09-17:16-17-20  Normal      4871215641    151          2         2
```

Display detailed statistics about eMDI instance 3 that monitors UDP flows.

```
<HUAWEI> display emdi statistics instance 3 verbose
Instance ID : 3       Monitor Period(s) : 10    Protocol : UDP
------------------------------------------------------------------------------
Originated From Slot 0
Record Time       : 2018-09-17:17-02-00   Monitor Status    : Abnormal
Received Packets  : 3850                  Rate pps          : 128
Received Bytes    : 5390000               Rate bps          : 1437333
Lost Packets      : 32261                 RTP-LR(1/100000)  : 89338
Disordered Packets: 0                     RTP-SER(1/100000) : 0
RTP-LP            : 35                    Average Jitter(us): 8540
Maximum Jitter(us): 8815                  Minimum Jitter(us)  : 8262
```

Display detailed statistics about eMDI instance 4 that monitors TCP flows.

```
<HUAWEI> display emdi statistics instance 4 verbose
Instance ID : 4       Monitor Period(s) : 10    Protocol : TCP
------------------------------------------------------------------------------
Originated From Slot 0
Record Time       : 2018-09-17:15-27-00   Monitor Status : Normal
Received Packets : 95                     Rate pps       : 9
Received Bytes   : 12510                  Rate bps(MFR)  : 10008
UPLC             : 0                      UPLR(1/100000) : 0
DPLC             : 0                      DPLR(1/100000) : 0
DRTT(us)         : 8396412
```

Display exception statistics about eMDI instance 5 that monitors UDP flows.

```
<HUAWEI> display emdi statistics instance 5 abnormal
Instance ID : 5       Monitor Period(s) : 30    Protocol : UDP
------------------------------------------------------------------------------
Originated From Slot 0
Record Time       : 2018-09-17:17-02-00   Monitor Status    : Abnormal
Received Packets  : 3850                  Rate pps          : 128
Received Bytes    : 5390000               Rate bps          : 1437333
Lost Packets      : 32261                 RTP-LR(1/100000)  : 89338
Disordered Packets: 0                     RTP-SER(1/100000) : 0
RTP-LP            : 35                    Average Jitter(us): 8540
Maximum Jitter(us): 8815                  Minimum Jitter(us)  : 8262
```

Display exception statistics about eMDI instance 6 that monitors TCP flows.

```
<HUAWEI> display emdi statistics instance 6 abnormal
Instance ID : 6       Monitor Period(s) : 30    Protocol : TCP
```



```
--------------------------------------------------------------------------------
Originated From Slot 0
Record Time      : 2018-09-17:15-27-00   Monitor Status : Abnormal
Received Packets : 95                    Rate pps       : 9
Received Bytes   : 12510                 Rate bps(MFR)  : 10008
UPLC             : 95                  UPLR(1/100000) : 100000
DPLC             : 0                   DPLR(1/100000) : 0
DRTT(us)         : 8396412
```

Table 16-94 Description of the **display emdi statistics instance** command output

Item	Description
Instance ID	ID of an eMDI instance.
Monitor Period(s)	Monitoring interval of an eMDI instance.
Protocol	Transport layer protocol.
Record Time	Time when a record is generated.
Monitor Status	Status of an eMDI instance: • Normal • Abnormal. This problem is caused by loss of packets to be sent to the CPU on the eMDI-enabled switch.
RTP-LR(1/100000)	Packet loss rate of RTP packets.
RTP-SER(1/100000)	Out-of-order rate of RTP packets.
Jitter(us)	Jitter of RTP packets.
MFR(bps)	Average bit rate.
DPLR(1/100000)	Downstream packet loss rate.
UPLR(1/100000)	Upstream packet loss rate.
DRTT(us)	Average downstream two-way delay, in microseconds.
Originated From Slot	ID of the slot where the card having eMDI instance started is located.
Received Packets	Number of the received packets.
Rate pps	Rate at which packets are received, in pps.
Received Bytes	Total number of received bytes.
Rate bps	Rate at which packets are received, in bps.
Lost Packets	Number of lost packets.
Disordered Packets	Number of out-of-order packets.

Item	Description
RTP-LP	Maximum number of consecutively lost RTP packets.
Average Jitter(us)	Average jitter, in microseconds.
Maximum Jitter(us)	Maximum jitter, in microseconds.
Minimum Jitter(us)	Minimum jitter, in microseconds.
Rate bps(MFR)	Average rate at which packets are received, in bps.
UPLC	Number of the lost upstream packets.
DPLC	Number of the lost downstream packets.

16.17.4 emdi

Function

The **emdi** command enables the eMDI function and displays the eMDI view.

The **undo emdi** command disables the eMDI function.

By default, the eMDI function is disabled.

Format

emdi

undo emdi

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To use eMDI to monitor network quality and demarcate faults, you must run this command to enable eMDI before performing other related operations.

Example

Enable the eMDI function.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi]
```

16.17.5 alarm threshold

Function

The **alarm threshold** command configures an alarm threshold for an eMDI instance.

The **undo alarm threshold** command restores the default alarm threshold for an eMDI instance.

By default, the alarm threshold for an eMDI instance is 100.

Format

alarm { **rtp-lr** | **rtp-ser** | **dplr** | **uplr** } **threshold** *threshold-value*

undo alarm { **rtp-lr** | **rtp-ser** | **dplr** | **uplr** } **threshold** [*threshold-value*]

Parameters

Parameter	Description	Value
rtp-lr	Specifies the alarm threshold of the packet loss rate for RTP packets (transported over UDP).	-
rtp-ser	Specifies the alarm threshold of the out-of-order rate for RTP packets (transported over UDP).	-
dplr	Specifies the alarm threshold of the downstream TCP packet loss rate.	-
uplr	Specifies the alarm threshold of the upstream TCP packet loss rate.	-
threshold *threshold-value*	Specifies the alarm threshold value.	The value is an integer in the range from 1 to 100000 (unit: 1/100,000).

Views

eMDI instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When eMDI is used to monitor quality and demarcate faults of video or audio services, you can run this command to configure the alarm threshold for an eMDI instance. When an indicator such as the out-of-order packet rate or packet loss rate monitored by the eMDI instance reaches the threshold for three consecutive times, an alarm is reported to the NMS. If the indicator no longer reaches the threshold within the following 60 consecutive monitoring intervals, the alarm is automatically cleared.

The switch supports alarms about the packet loss rate, out-of-order rate, and multi-flow detection for RTP packets (transported over UDP), as well as the downstream and upstream TCP packet loss rates. If the out-of-order rate of RTP packets transported over UDP is higher than the packet loss rate, the eMDI instance determines that multiple flows exist.

Prerequisites

A target flow has been configured in the eMDI instance using the **flow ipv4 udp** command or **flow ipv4 tcp** command.

Precautions

After an eMDI instance is started using the **start** command, the alarm threshold for the eMDI instance cannot be modified. To modify the alarm threshold, run the **stop** command to stop the eMDI instance first.

Example

Set the alarm threshold of the downstream packet loss rate to 1000 in eMDI instance 1.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 1
[HUAWEI-emdi-instance-1] flow ipv4 tcp source 10.0.0.1 destination 10.2.2.2
[HUAWEI-emdi-instance-1] alarm dplr threshold 1000
```

16.17.6 emdi instance

Function

The **emdi instance** command creates an eMDI instance and displays the eMDI instance view. If an eMDI instance has been created, the system displays the view of the eMDI instance.

The **undo emdi instance** command deletes a specified eMDI instance.

By default, no eMDI instance is created.

Format

emdi instance *instance-id*

undo emdi instance *instance-id*

Parameters

Parameter	Description	Value
instance-id	Specifies the ID of an eMDI instance to be created.	The value is an integer in the range from 1 to 4096.

Views

eMDI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An eMDI instance is a basic unit for eMDI to collect statistics about target flows. Each eMDI instance is composed of multiple elements, such as the target flow and monitoring interval. After the eMDI function is enabled, you must run this command to create an eMDI instance for quality monitoring and fault demarcation of video or audio services.

Precautions

- You can create one or more eMDI instances. The number of eMDI instances that can concurrently run a device depends on the product model, which can be queried using the **display emdi** command.
- An eMDI instance can monitor only one target flow.

Example

Create an eMDI instance with the ID of 1.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 1
[HUAWEI-emdi-instance-1]
```

16.17.7 monitor-period

Function

The **monitor-period** command sets the monitoring interval of an eMDI instance.

The **undo monitor-period** command restores the default monitoring interval of an eMDI instance.

By default, the monitoring interval of an eMDI instance is 60 seconds.

Format

monitor-period *period-value*

undo monitor-period [*period-value*]

Parameters

Parameter	Description	Value
period-value	Specifies the monitoring interval of an eMDI instance.	The value is of the enumerated type and can be set to 10, 30, or 60, in seconds.

Views

eMDI instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When eMDI is used to monitor quality and demarcate faults of video or audio services, an eMDI instance obtains monitoring data from the device at a specified interval.

Precautions

After an eMDI instance is started, its monitoring interval cannot be modified. To modify the monitoring interval, run the **stop** command to stop the eMDI instance first.

Example

Set the monitoring interval of eMDI instance 1 to 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 1
[HUAWEI-emdi-instance-1] monitor-period 10
```

16.17.8 end lifetime

Function

The **end lifetime** command sets the lifetime of an eMDI instance.

The **undo end lifetime** command restores the default lifetime of an eMDI instance.

By default, the lifetime of an eMDI instance is 1 hour.

Format

end lifetime { **seconds** *seconds* | **minutes** *minutes* | **hours** *hours* | **days** *days* }

undo end lifetime [**seconds** *seconds* | **minutes** *minutes* | **hours** *hours* | **days** *days*]

Parameters

Parameter	Description	Value
seconds *seconds*	Specifies the lifetime of an eMDI instance, in seconds.	The value is an integer in the range from 300 to 604800.
minutes *minutes*	Specifies the lifetime of an eMDI instance, in minutes.	The value is an integer in the range from 5 to 10080.
hours *hours*	Specifies the lifetime of an eMDI instance, in hours.	The value is an integer in the range from 1 to 168.
days *days*	Specifies the lifetime of an eMDI instance, in days.	The value is an integer in the range from 1 to 7.

Views

eMDI instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

eMDI is a one-off monitoring activity and does not need to run for a long time. You can run this command to configure the lifetime of an eMDI instance. After the eMDI instance is started, it stops automatically when its lifetime expires.

Precautions

After an eMDI instance is started, its lifetime cannot be modified. To modify the lifetime, run the **stop** command to stop the eMDI instance first.

Example

Set the lifetime of eMDI instance 1 to 300 seconds.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 1
[HUAWEI-emdi-instance-1] end lifetime seconds 300
```


16.17.9 flow ipv4 tcp

Function

The **flow ipv4 tcp** command configures a target TCP flow to be monitored by an eMDI instance.

The **undo flow ipv4 tcp** command deletes a target TCP flow monitored by an eMDI instance.

By default, no target flow is configured in an eMDI instance.

Format

flow ipv4 tcp source *source-ip-address* **destination** *destination-ip-address* [**vlan** *vlan-id* | **source-port** *source-port-number* | **destination-port** *destination-port-number*]*

undo flow ipv4 tcp source *source-ip-address* **destination** *destination-ip-address* [**vlan** *vlan-id* | **source-port** *source-port-number* | **destination-port** *destination-port-number*]*

undo flow

Parameters

Parameter	Description	Value
source *source-ip-address*	Specifies the source IP address of a target flow.	The value is in dotted decimal notation.
destination *destination-ip-address*	Specifies the destination IP address of a target flow.	The value is in dotted decimal notation.
vlan *vlan-id*	Specifies the VLAN ID of a target flow.	The value is an integer in the range from 1 to 4094.
source-port *source-port-number*	Specifies the source port number of a target flow.	The value is an integer in the range from 1 to 65535.
destination-port *destination-port-number*	Specifies the destination port number of a target flow.	The value is an integer in the range from 1 to 65535.

Views

eMDI instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As a key element in an eMDI instance, a target flow to be monitored must be configured before the eMDI instance is started.

A target flow is the object monitored by an eMDI instance, and can be defined by any combinations of multiple attributes such as source IP address, destination IP address, VLAN ID, source port number, and destination port number. Specifying more attributes makes the target flow more accurate. Therefore, it is recommended that you specify more attributes to improve precision of monitoring results.

Precautions

- An eMDI instance can monitor only one target flow. If multiple target flows are configured in an eMDI instance, only the last configured one takes effect.
- In a video surveillance scenario, specify the number of the port connected to IPCs to ensure uniqueness of the target flow. Otherwise, the monitoring results will be affected in multi-flow scenarios.
- After an eMDI instance is started, the target flow monitored by the eMDI instance cannot be modified. To modify the target flow, run the **stop** command to stop the eMDI instance first.
- If 0.0.0.0 is specified by **source** *source-ip-address* or **destination** *destination-ip-address*, the source or destination IP address of the target flow can be any IP address. Examples are as follows:
  - If *source-ip-address* is set to 0.0.0.0 and *destination-ip-address* is set to 10.1.1.1, flows sourced from any IP address and destined for 10.1.1.1 are monitored.
  - If *source-ip-address* is set to 10.1.1.1 and *destination-ip-address* is set to 0.0.0.0, flows sourced from 10.1.1.1 and destined for any IP address are monitored.
  - If both *source-ip-address* and *destination-ip-address* are set to 0.0.0.0, the system does not check the source or destination IP addresses of the target flow to be monitored.

Example

Set the source and destination IP addresses of the target TCP flow to be monitored by eMDI instance 2 to 10.0.0.1 and 10.0.0.2, respectively.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 2
[HUAWEI-emdi-instance-2] flow ipv4 tcp source 10.0.0.1 destination 10.0.0.2
```

16.17.10 flow ipv4 udp

Function

The **flow ipv4 udp** command configures a target UDP flow to be monitored by an eMDI instance.

The **undo flow ipv4 udp** command deletes the target UDP flow monitored by an eMDI instance.

By default, no target flow is configured in an eMDI instance.

Format

flow ipv4 udp source *source-ip-address* **destination** *destination-ip-address* [**vlan** *vlan-id* | **source-port** *source-port-number* | **destination-port** *destination-port-number* | **pt** *pt-value* | **clock-rate** *clock-rate-value*]*

undo flow ipv4 udp source *source-ip-address* **destination** *destination-ip-address* [**vlan** *vlan-id* | **source-port** *source-port-number* | **destination-port** *destination-port-number* | **pt** *pt-value* | **clock-rate** *clock-rate-value*]*

undo flow

Parameters

Parameter	Description	Value
source *source-ip-address*	Specifies the source IP address of a target flow.	The value is in dotted decimal notation.
destination *destination-ip-address*	Specifies the destination IP address of a target flow.	The value is in dotted decimal notation.
vlan *vlan-id*	Specifies the VLAN ID of a target flow.	The value is an integer in the range from 1 to 4094.
source-port *source-port-number*	Specifies the source port number of a target flow.	The value is an integer in the range from 1 to 65535.
destination-port *destination-port-number*	Specifies the destination port number of a target flow.	The value is an integer in the range from 1 to 65535.
pt *pt-value*	Specifies the payload type of a target flow.	The value is an integer in the range from 25 to 127.
clock-rate *clock-rate-value*	Specifies the clock rate of a target flow.	The value is of the enumerated type and can be set to 8000, 16000, or 90000, in Hz. The default value is 90000.

Views

eMDI instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As a key element in an eMDI instance, a target flow to be monitored must be configured before the eMDI instance is started.

A target flow is the object monitored by eMDI, and can be defined by any combinations of multiple attributes such as source IP address, destination IP address, VLAN ID, source port number, and destination port number. Specifying more attributes makes the target flow more accurate. Therefore, it is recommended that you specify more attributes to improve precision of monitoring results.

Precautions

- An eMDI instance can monitor only one target flow. If multiple target flows are configured in an eMDI instance, only the last configured one takes effect.
- In a video surveillance scenario, specify the number of the port connected to IPCs to ensure uniqueness of the target flow. Otherwise, the monitoring results will be affected in multi-flow scenarios.
- In an IPTV scenario, specify the **pt** *pt-value* parameter to ensure uniqueness of a target flow. Otherwise, the monitoring results will be affected in multi-flow scenarios.
- After an eMDI instance is started, the target flow monitored by the eMDI instance cannot be modified. To modify the target flow, run the **stop** command to stop the eMDI instance first.

Example

Set the source and destination IP addresses of the target UDP flow to be monitored by eMDI instance 1 to 10.0.0.1 and 10.0.0.2, respectively.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 1
[HUAWEI-emdi-instance-1] flow ipv4 udp source 10.0.0.1 destination 10.0.0.2
```

16.17.11 reset emdi statistics instance

Function

The **reset emdi statistics instance** command clears the statistics about an eMDI instance.

Format

reset emdi statistics instance *instance-id*

Parameters

Parameter	Description	Value
instance-id	Specifies the ID of an eMDI instance.	The value is an integer that ranges from 1 to 5120 for S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S, and from 1 to 4112 for other models.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To obtain the latest monitoring results of an eMDI instance, you can run this command to clear historical monitoring results of the eMDI instance, and then run the **display emdi statistics instance** command to obtain the latest ones.

Example

Clear statistics about eMDI instance 1.

```
<HUAWEI> reset emdi statistics instance 1
```

16.17.12 start

Function

The **start** command starts an eMDI instance.

Format

start

Parameters

None

Views

eMDI instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an eMDI instance is created and a target flow is configured, you can run this command to start the eMDI instance to monitor quality and demarcate faults of video or audio services.

Prerequisites

A target flow has been configured for an eMDI instance using the **flow ipv4 tcp** or **flow ipv4 udp** command.

Precautions

After an eMDI instance is started, all parameters in the eMDI instance cannot be modified. To modify the parameters, run the **stop** command to stop the eMDI instance first.

Example

Start eMDI instance 1.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 1
[HUAWEI-emdi-instance-1] flow ipv4 udp source 10.0.0.1 destination 10.0.0.2
[HUAWEI-emdi-instance-1] start
```

16.17.13 stop

Function

The **stop** command stops an eMDI instance immediately.

Format

stop

Parameters

None

Views

eMDI instance view

Default Level

2: Configuration level

Usage Guidelines

You can stop an eMDI instance in either of the following situations:

- Stop execution of the eMDI instance immediately.
- Modify the target flow, monitoring interval, lifetime, or alarm threshold of the eMDI instance.

Example

Stop eMDI instance 1.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] emdi instance 1
[HUAWEI-emdi-instance-1] stop
```

16.17.14 stop all

Function

The **stop all** command stops all eMDI instances immediately.

Format

stop all

Parameters

None

Views

eMDI view

Default Level

2: Configuration level

Usage Guidelines

If eMDI instances have completed fault demarcation before their lifetime expires, you can run this command to stop all the eMDI instances.

Example

Stop all eMDI instances.

```
<HUAWEI> system-view
[HUAWEI] emdi
[HUAWEI-emdi] stop all
```