3Com Switch 4210G Family

Command Reference Guide

Switch 4210G 24-Port

Switch 4210G 48-Port

Switch 4210G NT 24-Port

Switch 4210G NT 48-Port

Switch 4210G PWR 24-Port

Switch 4210G PWR 48-Port

Product Version:
Release 2202
Manual Version:
6W100-20100205
www.3com.com

3Com Corporation
350 Campus Drive, Marlborough,
MA, USA 01752 3064

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

About This Manual

Organization

3Com Switch 4210G Family Command Reference Guide is organized as follows:

Volume	Features			
00-Command Index	Command Index			
01-Access Volume	Ethernet Port	Link Aggregation	Port Isolation	MSTP
	LLDP	VLAN	Isolate-User-VLAN	Voice VLAN
	GVRP	QinQ	BPDU Tunneling	Port Mirroring
02-IP Services Volume	IP Addressing	ARP	Proxy ARP	ARP Attack Defense
	DHCP Relay Agent	DHCP Client	DHCP Snooping	BOOTP Client
	DNS	IP Performance Optimization	UDP Helper	IPv6 Basics
	sFlow			
03-IP Routing Volume	IP Routing Table	Static Routing	IPv6 Static Routing	
04-Multicast Volume	IGMP Snooping	Multicast VLAN	MLD Snooping	IPv6 Multicast VLAN
05-QoS Volume	QoS Policy	Priority Mapping	Traffic Shaping and Line Rate	Congestion Management
	Traffic Mirroring	User Profile		
06-Security Volume	AAA	RADIUS	HWTACACS	802.1X
	EAD Fast Deployment	HABP	MAC Authentication	Port Security
	IP Source Guard	SSH2.0	PKI	SSL
	Public Key	ACL		
07-High Availability Volume	Smart Link	Monitor Link	RRPP	DLDP
	Ethernet OAM	Connectivity Fault Detection	Track	
08-System Volume	Logging into an Ethernet Switch	Controlling Login Users	Basic System Configuration	Device Management
	File System Management	FTP	TFTP	HTTP
	HTTPS	SNMP	MIB	RMON
	MAC Address Table Management	MAC Information Configuration	System Maintaining and Debugging	Information Center
	Hotfix	NQA	NTP	Cluster Management
	IRF	IPC	PoE	

Conventions

The manual uses the following conventions:

Command conventions

Convention	Description
Boldface	The keywords of a command line are in **Boldface**.
italic	Command arguments are in *italic*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. Many or none can be selected.
&<1-n>	The argument(s) before the ampersand (&) sign can be entered 1 to n times.
#	A line starting with the # sign is comments.

GUI conventions

Convention	Description
< >	Button names are inside angle brackets. For example, click <OK>.
[ ]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

Symbols

Convention	Description
 **Warning**	Means reader be extremely careful. Improper operation may cause bodily injury.
 **Caution**	Means reader be careful. Improper operation may cause data loss or damage to equipment.
 **Note**	Means a complementary description.

Related Documentation

In addition to this manual, each 3com Switch 4210G documentation set includes the following:

Manual	Description
3Com Switch 4210G Family Configuration Guide-Release 2202	Describe how to configure your 4210G Switch using the supported protocols and CLI commands.
3Com Switch 4210G Family Getting Started Guide	This guide provides all the information you need to install and use the 3Com Switch 4210G Family.

Obtaining Documentation

You can access the most up-to-date 3Com product documentation on the World Wide Web at this URL: http://www.3com.com.

Appendix A Command Index

The command index includes all the commands in the *Command Manual*, which are arranged alphabetically.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

Table of Contents

1 Ethernet Port Configuration Commands

Ethernet Port Configuration Commands

broadcast-suppression

Syntax

broadcast-suppression { *ratio* | **pps** *max-pps* }

undo broadcast-suppression

View

Ethernet port view, port group view

Default Level

2: System level

Parameters

ratio: Maximum percentage of broadcast traffic to the total transmission capability of an Ethernet port. The smaller the ratio, the less broadcast traffic is allowed to pass through the interface. this argument ranges from 1 to 100.

pps *max-pps*: Specifies the maximum number of broadcast packets that can be forwarded on an Ethernet port per second (in pps, representing packets per second).

- For a Gigabit port, the value range is 1 to 1488100.
- For a 10-Gigabit port, the value range is 1 to 14881000.

Note that:

- When a suppression granularity larger than 1 is specified on the device, the value of the **pps** keyword should be no smaller than and an integral multiple of the granularity. The broadcast suppression threshold value configured through this keyword on an Ethernet port may not be the one that actually takes effect. To display the actual broadcast suppression threshold value on an Ethernet port, you can use the **display interface** command.
- When no suppression granularity is specified or the suppression granularity is set to 1, the value of the **pps** keyword should be no smaller than 1, and the broadcast suppression threshold value is the one that actually takes effect on the Ethernet port.

Description

Use the **broadcast-suppression** command to set a broadcast traffic threshold on one or multiple Ethernet ports.

Use the **undo broadcast-suppression** command to restore the default.

By default, all broadcast traffic is allowed to pass through an Ethernet port, that is, broadcast traffic is not suppressed.

If you execute this command in Ethernet port view, the configuration takes effect only on the current interface. If you execute this command in port-group view, the configuration takes effect on all the ports in the port group.

When broadcast traffic exceeds the broadcast traffic threshold, the system begins to discard broadcast packets until the broadcast traffic drops below the threshold to ensure operation of network services.

 **Note**

- If you set different suppression ratios in Ethernet port view or port-group view for multiple times, the latest configuration takes effect.
- Do not use the **broadcast-suppression** command along with the **storm-constrain** command. Otherwise, the broadcast storm suppression ratio configured may get invalid.

Examples

For Ethernet port GigabitEthernet 1/0/1, allow broadcast traffic equivalent to 20% of the total transmission capability of GigabitEthernet 1/0/1 to pass.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] broadcast-suppression 20
```

For all the ports of the manual port group named **group1**, allow broadcast traffic equivalent to 20% of the total transmission capability of each port to pass and suppress excessive broadcast packets.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1] group-member GigabitEthernet 1/0/2
[Sysname-port-group-manual-group1] group-member GigabitEthernet 1/0/3
[Sysname-port-group-manual-group1] broadcast-suppression 20
```

description

Syntax

description *text*

undo description

View

Ethernet port view

Default Level

2: System level

Parameters

text: Description of an Ethernet port, a string of 1 to 80 characters. Currently, the device supports the following types of characters or symbols: standard English characters (numbers and case-sensitive

letters), special English characters, spaces, and other characters or symbols that conform to the Unicode standard.

 **Note**

- A port description can be the mixture of English characters and other Unicode characters. The mixed description cannot exceed the specified length.
- To use a type of Unicode characters or symbols in a port description, you need to install the corresponding Input Method Editor (IME) and log in to the device through remote login software that supports this character type.
- Each Unicode character or symbol (non-English characters) takes the space of two regular characters. When the length of a description string reaches or exceeds the maximum line width on the terminal software, the software starts a new line, possibly breaking a Unicode character into two. As a result, garbled characters may be displayed at the end of a line.

Description

Use the **description** command to set the description string of the current interface.

Use the **undo description** command to restore the default.

By default, the description of an interface is the interface name followed by the “interface” string, **GigabitEthernet1/0/1 Interface** for example.

Related commands: **display interface**.

Examples

Configure the description string of interface GigabitEthernet 1/0/1 as **lanswitch-interface**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] description lanswitch-interface
```

display brief interface

Syntax

display brief interface [*interface-type* [*interface-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type: Type of a specified interface.

interface-number: Number of a specified interface.

|: Uses a regular expression to filter output information. For detailed description on regular expression, refer to *Basic System Configuration* in the *System Volume*.

begin: Displays the line that matches the regular expression and all the subsequent lines.

exclude: Displays the lines that do not match the regular expression.

include: Displays the lines that match the regular expression.

regular-expression: Regular expression, a string of 1 to 256 characters. Note that this argument is case-sensitive.

Description

Use the **display brief interface** command to display brief interface information.

- If neither interface type nor interface number is specified, all interface information will be displayed.
- If only interface type is specified, then only information of this particular type of interface will be displayed.
- If both interface type and interface number are specified, then only information of the specified interface will be displayed.

Related commands: **interface**.

Examples

Display the brief information of interfaces.

```
<Sysname> display brief interface
The brief information of interface(s) under route mode:
Interface          Link     Protocol-link  Protocol type    Main IP
Loop1              UP       UP(spoofing)   LOOP           2.2.2.1
NULL0              UP       UP(spoofing)   NULL           --
Vlan1              UP       UP           ETHERNET       192.168.0.153
Vlan10             DOWN     DOWN          ETHERNET        1.1.1.1
Vlan100            ADM DOWN  DOWN          ETHERNET        --

The brief information of interface(s) under bridge mode:
Interface          Link     Speed       Duplex   Link-type  PVID
BAGG1              DOWN     auto        auto     access     1
GE1/0/1            DOWN     auto        auto     access     1
GE1/0/2            DOWN     auto        auto     access     1
GE1/0/3            DOWN     auto        auto     access     1
GE1/0/4            UP       1G(a)       full(a)  access     1
GE1/0/5            DOWN     auto        auto     access     1
GE1/0/6            DOWN     auto        auto     access     1
GE1/0/7            DOWN     auto        auto     access     1
GE1/0/8            DOWN     auto        auto     access     1
GE1/0/9            DOWN     auto        auto     access     1
GE1/0/10           DOWN     auto        auto     access     1
GE1/0/11           DOWN     auto        auto     trunk      1
GE1/0/12           DOWN     auto        auto     trunk      1
```

Display the information of interfaces beginning with the string “spoof”.

```
<Sysname> display brief interface | begin spoof
```

```
The brief information of interface(s) under route mode:
Interface          Link     Protocol-link  Protocol type    Main IP
Loop0              UP       UP(spoofing)   LOOP           5.5.5.5
NULL0              UP       UP(spoofing)   NULL           --
Vlan999            UP       UP           ETHERNET       10.1.1.1
```

Display the brief information of all UP interfaces.

```
<Sysname> display brief interface | include UP
The brief information of interface(s) under route mode:
Interface          Link     Protocol-link  Protocol type    Main IP
Loop0              UP      UP(spoofing)   LOOP           5.5.5.5
NULL0              UP      UP(spoofing)   NULL           --
Vlan999            UP      UP           ETHERNET       10.1.1.1

The brief information of interface(s) under bridge mode:
Interface          Link     Speed     Duplex   Link-type  PVID
GE1/0/7             UP      100M(a)    full(a)  trunk     303
GE1/0/9             UP      100M(a)    full(a)  access    999
```

Display the brief information of all interfaces excluding Ethernet ports.

```
<Sysname> display brief interface | exclude GE
The brief information of interface(s) under route mode:
Interface          Link     Protocol-link  Protocol type    Main IP
Loop1              UP       UP(spoofing)   LOOP           2.2.2.1
NULL0              UP       UP(spoofing)   NULL           --
Vlan1              UP       UP           ETHERNET       192.168.0.153
Vlan10             DOWN     DOWN          ETHERNET       1.1.1.1
Vlan100            ADM DOWN  DOWN          ETHERNET       --
The brief information of interface(s) under bridge mode:
Interface          Link     Speed       Duplex   Link-type  PVID
BAGG1              DOWN     auto        auto     access    1
```

Table 1-1 display brief interface command output description

Field	Description
The brief information of interface(s) under route mode:	Brief information of interface(s) in route mode
Interface	Abbreviated interface name
Link	Interface physical link state, which can be up or down
Protocol-link	Interface protocol link state, which can be up or down
Protocol type	Interface protocol type
The brief information of interface(s) under bridge mode:	Brief information of interface(s) in bridge mode
Speed	Interface rate, in bps

Field	Description
Duplex	Duplex mode, which can be half (half duplex), full (full duplex), or auto (auto-negotiation).
PVID	Default VLAN ID

display interface

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

interface-type: Type of a specified interface.

interface-number: Number of a specified interface.

Description

Use the **display interface** command to display the current state of a specified interface and related information.

- If neither interface type nor interface number is specified, all interface information will be displayed.
- If only interface type is specified, then only information of this particular type of interface will be displayed.
- If both interface type and interface number are specified, then only information of the specified interface will be displayed.

Related commands: **interface**.

Examples

Display the current state of interface GigabitEthernet 1/0/1 and related information.

```
<Sysname> display interface GigabitEthernet 1/0/1
 GigabitEthernet1/0/1 current state: DOWN
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e200-8048
 Description: GigabitEthernet1/0/1 Interface
 Loopback is not set
 Media type is twisted pair, port hardware type is 100_BASE_TX
 Unknown-speed mode, unknown-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 Flow-control is not enabled
 The Maximum Frame Length is 9216
 Broadcast MAX-ratio: 100%
 Unicast MAX-ratio: 100%
```

```
Multicast MAX-ratio: 100%
Allow jumbo frame to pass
PVID: 100
Mdi type: auto
Link delay is 0(sec)
Port link-type: access
 Tagged   VLAN ID : none
 Untagged VLAN ID : 100
Port priority: 0
Peak value of input: 96132560 bytes/sec, at 2007-10-26 07:05:06
Peak value of output: 0 bytes/sec, at 2000-04-26 12:00:12
Last 300 seconds input:  6 packets/sec 678 bytes/sec    20%
Last 300 seconds output:  1 packets/sec 179 bytes/sec    17%
Input (total):  61745144 packets, 12152212250 bytes
        0 unicasts, 47519150 broadcasts, 12121681 multicasts
Input (normal):  61745144 packets, - bytes
        205227373 unicasts, 47519150 broadcasts, 12121681 multicasts
Input:  0 input errors, 0 runts, 0 giants, 0 throttles
        0 CRC, 0 frame, - overruns, 0 aborts
        - ignored, - parity errors
Output (total): 1395522 packets, 183608303 bytes
        0 unicasts, 13 broadcasts, 1273860 multicasts, 0 pauses
Output (normal): 1395522 packets, - bytes
        0 unicasts, 13 broadcasts, 1273860 multicasts, 0 pauses
Output: 0 output errors, - underruns, - buffer failures
        0 aborts, 0 deferred, 0 collisions, 0 late collisions
        0 lost carrier, - no carrier
```

Table 1-2 display interface command output description

Field	Description
GigabitEthernet1/0/1 current state	Current physical link state of the Ethernet port
IP Packet Frame Type	Frame type of the Ethernet port
Description	Description of the interface
Unknown-speed mode	Unknown-speed mode, in which mode speed is negotiated between the current host and the peer.
unknown-duplex mode	Unknown-duplex mode, in which mode speed is negotiated between the current host and the peer.
The Maximum Frame Length	The maximum frame length allowed on an interface
Broadcast MAX-ratio	Broadcast storm suppression ratio (the maximum ratio of allowed number of broadcast packets to overall traffic through an interface)
Unicast MAX-ratio	Unicast storm suppression ratio (the maximum ratio of allowed number of unknown unicast packets to overall traffic over an interface)

Field	Description
Multicast MAX-ratio	Multicast storm suppression ratio (the maximum ratio of allowed number of multicast packets to overall traffic through an interface)
PVID	Default VLAN ID
Mdi type	Cable type
Link delay	The suppression time of physical-link-state changes
Port link-type	Interface link type, which could be access, trunk, and hybrid.
Tagged VLAN ID	VLANs whose packets are sent through the port with VLAN tag kept
Untagged VLAN ID	VLANs whose packets are sent through the port with VLAN tag stripped off
Peak value of input	Peak value of inbound traffic, in bytes/sec.
Peak value of output	Peak value of outbound traffic, in bytes/sec.
Last 300 seconds input: 0 packets/sec 0 bytes/sec Last 300 seconds output: 0 packets/sec 0 bytes/sec	Average rate of input and output traffic in the last 300 seconds, in pps and Bps
Input (total): 61745144 packets, 12152212250 bytes 0 unicasts, 47519150 broadcasts, 12121681 multicasts	Packet statistics on the inbound direction of the interface, including the statistics of normal packets,and abnormal packets, in packets and bytes Number of unicast packets, broadcast packets, and multicast packets on the inbound direction of the interface
Input (normal): 61745144 packets, - bytes 205227373 unicasts, 47519150 broadcasts, 12121681 multicasts	Normal packet statistics on the inbound direction of the interface, including the statistics of normal packets in packets and bytes Number of unicast packets, broadcast packets, and multicast packets on the inbound direction of the interface.
input errors	Input packets with errors
runts	Frames received that were shorter than 64 bytes, yet in correct formats, and contained valid CRCs
giants	Frames received that were longer than the maximum frame length supported on the interface: • For an Ethernet interface that permits jumbo frames, giants refer to frames that are longer than 9212 bytes (without VLAN tags) or 9216 bytes (with VLAN tags). • For an Ethernet interface that forbids jumbo frames, giants refer to frames that are longer than 1522 bytes (without VLAN tags) or 1526 bytes (with VLAN tags)
throttles	The number of times the receiver on the interface was disabled, possibly because of buffer or CPU overload
CRC	Total number of packets received that had a normal length, but contained checksum errors
frame	Total number of frames that contained checksum errors and a non-integer number of bytes
- overruns	Number of times the receive rate of the interface exceeded the capacity of the input queue, causing packets to be discarded

Field	Description
aborts	Total number of illegal packets received, including: • Fragment frames: Frames that were shorter than 64 bytes (with an integral or non-integral length) and contained checksum errors • Jabber frames: Frames that were longer than the maximum frame length supported on the Ethernet interface and contained checksum errors (the frame lengths in bytes may or may not be integers). For an Ethernet interface that permits jumbo frames, jabber frames refer to frames that are longer than 9212 bytes (without VLAN tags) or 9216 bytes (with VLAN tags) and contain checksum errors; for an Ethernet interface that forbids jumbo frames, jabber frames refer to frames that are longer than 1522 bytes (without VLAN tags) or 1526 bytes (with VLAN tags) and contain checksum errors. • Symbol error frames: Frames that contained at least one undefined symbol • Unknown operation code frames: Frames that were MAC control frames but not pause frames • Length error frames: Frames whose 802.3 length fields did not match the actual frame lengths (46 bytes to 1500 bytes)
- ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers
- parity errors	Total number of frames with parity errors
Output (total): 1395522 packets, 183608303 bytes 0 unicasts, 13 broadcasts, 1273860 multicasts, 0 pauses	Packet statistics on the outbound direction of the interface, including the statistics of normal packets, abnormal packets, and normal pause frames, in packets and bytes Number of unicast packets, broadcast packets, multicast packets, and pause frames on the outbound direction of the interface
Output (normal): 1395522 packets, - bytes 0 unicasts, 13 broadcasts, 1273860 multicasts, 0 pauses	Normal packet statistics on the outbound direction of the interface, including the statistics of normal packets and pause frames, in packets and bytes Number of unicast packets, broadcast packets, multicast packets, and pause frames on the outbound direction of the interface.
output errors	Output packets with errors
- underruns	Number of times the transmit rate of the interface exceeded the capacity of the output queue, causing packets to be discarded. This is a very rare hardware-related problem.
- buffer failures	Number of packets dropped because the interface ran low on output buffers
aborts	Number of packets that failed to be transmitted due to causes such as Ethernet collisions
deferred	Number of frames whose first transmission attempt was delayed, due to traffic on the network media, and that were successfully transmitted later
collisions	Number of times frames were delayed due to Ethernet collisions detected during the transmission
late collisions	Number of times frames were delayed due to the detection of collisions after the first 512 bits of the frames were already on the network

Field	Description
lost carrier	Number of times the carrier was lost during transmission. This counter applies to serial WAN interfaces.
- no carrier	Number of times the carrier was not present in the transmission. This counter applies to serial WAN interfaces.

Note

"**-**" indicates that the corresponding entry is not supported.

display loopback-detection

Syntax

display loopback-detection

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display loopback-detection** command to display loopback detection information on a port.

If loopback detection is already enabled, this command will also display the detection interval and information on the ports currently detected with a loopback.

Examples

Display loopback detection information on a port.

```
<Sysname> display loopback-detection
Loopback-detection is running
Detection interval time is 30 seconds
No port is detected with loopback
```

Table 1-3 display loopback-detection command output description

Field	Description
Loopback-detection is running	Loopback-detection is running.
Detection interval time is 30 seconds	Detection interval is 30 seconds.
No port is detected with loopback	No port is currently being detected with a loopback.

display packet-drop interface

Syntax

display packet-drop interface [*interface-type* [*interface-number*]]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type: Type of a specified interface.

interface-number: Number of a specified interface.

Description

Use the **display packet-drop interface** command to display information about dropped packets on an interface or multiple interfaces.

- If you do not specify an interface type or interface number, this command displays information about dropped packets on all the interfaces on the device.
- If you specify an interface type only, this command displays information about dropped packets on the specified type of interfaces.
- If you specify both the interface type and interface number, this command displays information about dropped packets on the specified interface.

Examples

Display information about dropped packets on GigabitEthernet 1/0/1.

```
<Sysname> display packet-drop interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1:
Packets dropped by GBP full or insufficient bandwidth: 301
Packets dropped by FFP: 261
Packets dropped by STP non-forwarding state: 321
```

display packet-drop summary

Syntax

display packet-drop summary

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display packet-drop summary** command to display information about dropped packets on all interfaces.

Examples

Display information about dropped packets on all interfaces.

```
<Sysname> display packet-drop summary
All interfaces:
Packets dropped by GBP full or insufficient bandwidth: 301
Packets dropped by FFP: 261
Packets dropped by STP non-forwarding state: 321
Packets dropped by Rate-limit: 143
```

Table 1-4 display packet-drop summary command output description

Field	Description
Packets dropped by GBP full or insufficient bandwidth	Packets that are dropped because the buffer is used up or the bandwidth is insufficient
Packets dropped by FFP	Packets that are filtered out
Packets dropped by STP non-forwarding state	Packets that are dropped because STP is in the non-forwarding state

display port combo

Syntax

display port combo

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display port combo** command to display the Combo ports of a device and the corresponding optical ports and electrical ports.

Examples

Display the Combo ports of the device and the corresponding optical ports and electrical ports.

```
<Sysname> display port combo
Combo-group        Active                  Inactive
      1       GigabitEthernet1/0/45      GigabitEthernet1/0/51
      2       GigabitEthernet1/0/46      GigabitEthernet1/0/49
```

```
3       GigabitEthernet1/0/47      GigabitEthernet1/0/52
4       GigabitEthernet1/0/48      GigabitEthernet1/0/50
```

Table 1-5 display port combo command output description

Field	Description
Combo-group	Combo ports of the device, represented by Combo port number, which is generated by the system.
Active	Ports of the Combo ports that are active
Inactive	Ports of the Combo ports that are inactive

As for the optical port and the electrical port of a Combo port, the one with the smaller port number is active by default. You can determine whether a port is an optical port or an electrical port by checking the “Media type is” field of the **display interface** command.

display port-group manual

Syntax

display port-group manual [**all | name** *port-group-name*]

View

Any view

Default Level

2: System level

Parameters

all: Specifies all the manual port groups.

name *port-group-name*: Specifies the name of a manual port group, a string of 1 to 32 characters.

Description

Use the **display port-group manual** command to display the information about a manual port group or all the manual port groups.

- If you provide the *port-group-name* argument, this command displays the details for a specified manual port group, including its name and the Ethernet port ports included.
- If you provide the **all** keyword, this command displays the details for all manual port groups, including their names and the Ethernet port ports included.
- Absence of parameters indicates that the names of all the port groups will be displayed.

Examples

Display the names of all the port groups.

```
<Sysname> display port-group manual
The following manual port group exist(s):
group1                              group2
```

Display details of all the manual port groups.

```
<Sysname> display port-group manual all
```

```
Member of group1:
   GigabitEthernet1/0/3          GigabitEthernet1/0/4          GigabitEthernet1/0/5
   GigabitEthernet1/0/6          GigabitEthernet1/0/7          GigabitEthernet1/0/8

Member of group2:
None
```

Table 1-6 display port-group manual command output description

Field	Description
Member of group	Member of the manual port group

display storm-constrain

Syntax

display storm-constrain [**broadcast** | **multicast**] [**interface** *interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

broadcast: Displays the information about storm constrain for broadcast packets.

multicast: Displays the information about storm constrain for multicast packets.

interface *interface-type interface-number*: Specifies an interface by its type and number.

Description

Use the **display storm-constrain** command to display the information about storm constrain.

If you provide no argument or keyword, this command displays the information about storm constrain for all types of packets on all the interfaces.

Examples

Display the information about storm constrain for all types of packets on all the interfaces.

```
<Sysname> display storm-constrain
Abbreviation: BC - broadcast; MC - multicast; UC - unicast
 Flow Statistic Interval: 10(second)
PortName     Type LowerLimit UpperLimit CtrMode  Status  Trap Log SwiNum Unit
--------------------------------------------------------------------------------
GE1/0/2      BC   1          2          N/A     normal  on   on  0     kbps
GE1/0/2      MC   1          5          N/A     normal  on   on  0     ratio
```

Table 1-7 display storm-constrain command output description

Field	Description
Flow Statistic Interval	Interval for generating storm constrain statistics

Field	Description
PortName	Abbreviated port name
Type	Type of the packets for which storm constrain function is enabled, which can be broadcast (for broadcast packets), and multicast (for multicast packets).
LowerLimit	Lower threshold (in pps, Kbps or percentage)
UpperLimit	Upper threshold (in pps, Kbps or percentage)
CtrMode	Action to be taken when the upper threshold is reached, which can be block, shutdown, and N/A.
Status	Interface state, which can be normal (indicating the interface operates properly), control (indicating the interface is blocked or shut down).
Trap	State of trap messages sending. “on” indicates trap message sending is enabled; “off” indicates trap message sending is disabled.
Log	State of log sending. “on” indicates log sending is enabled; “off” indicates log sending is disabled.
SwiNum	Number of the forwarding state switching. This field is numbered modulo 65,535.

duplex

Syntax

duplex { **auto** | **full** | **half** }

undo duplex

View

Ethernet port view

Default Level

2: System level

Parameters

auto: Indicates that the interface is in auto-negotiation state.

full: Indicates that the interface is in full-duplex state.

half: Indicates that the interface is in half-duplex state. The optical interfaces of SFP ports and the electrical interfaces of Ethernet ports whose port rate is configured as 1000 Mbps do not support the **half** keyword.

Description

Use the **duplex** command to configure the duplex mode for an Ethernet port.

Use the **undo duplex** command to restore the duplex mode for an Ethernet port to the default.

By default, the duplex mode for an Ethernet port is **auto**.

Related commands: **speed**.

Note

10-Gigabit Ethernet ports do not support this command.

Examples

Configure the interface GigabitEthernet 1/0/1 to work in full-duplex mode.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] duplex full
```

flow-control

Syntax

flow-control

undo flow-control

View

Ethernet port view

Default Level

2: System level

Parameters

None

Description

Use the **flow-control** command to enable flow control on an Ethernet port.

Use the **undo flow-control** command to disable flow control on an Ethernet port.

By default, flow control on an Ethernet port is disabled.

Note

The flow control function takes effect on the local Ethernet port only when it is enabled on both the local and peer devices.

Examples

Enable flow control on interface GigabitEthernet1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname- GigabitEthernet1/0/1] flow-control
```

flow-interval

Syntax

flow-interval *interval*

undo flow-interval

View

Ethernet port view

Default Level

2: System level

Parameters

interval: Interval at which the interface collects statistics. It ranges from 5 to 300 seconds and must be a multiple of 5. The default value is 300 seconds.

Description

Use the **flow-interval** command to configure the time interval for collecting interface statistics.

Use the **undo flow-interval** command to restore the default interval.

Examples

Set the time interval for collecting interface statistics to 100 seconds.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] flow-interval 100
```

group-member

Syntax

group-member *interface-list*

undo group-member *interface-list*

View

Port group view

Default Level

2: System level

Parameters

interface-list: Ethernet port list, in the form of *interface-type interface-number* [**to** *interface-type interface-number*] &<1-10>, where &<1-10> indicates that you can specify up to 10 port or port ranges.

Description

Use the **group-member** command to assign an Ethernet port or a list of Ethernet ports to the manual port group.

Use the **undo group-member** command to remove an Ethernet port or a list of Ethernet ports from the manual port group.

By default, there is no Ethernet port in a manual port group.

Examples

Add interface GigabitEthernet 1/0/1 to the manual port group named **group1**.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1] group-member GigabitEthernet 1/0/1
```

interface

Syntax

interface *interface-type interface-number*

View

System view

Default Level

2: System level

Parameters

interface-type interface-number: Interface type and interface number.

Description

Use the **interface** command to enter interface view.

Examples

Enter GigabitEthernet 1/0/1 interface view

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1]
```

jumboframe enable

Syntax

jumboframe enable

undo jumboframe enable

View

Ethernet port view, port group view

Default Level

2: System level

Parameters

.None

Description

Use the **jumboframe enable** command to allow jumbo frames with the length of 9216 bytes to pass through an Ethernet port.

Use the **undo jumboframe enable** command to prevent frames longer than 1522 bytes from passing through an Ethernet port.

By default, the device allows frames no larger than 9216 bytes to pass through an Ethernet port.

You can configure length of jumbo frames on a port (in Ethernet port view, port-group view) to allow them to pass through Ethernet ports.

- Execution of this command under Ethernet port view will only apply the configurations to the current Ethernet port.
- Execution of this command under port group view will apply the configurations to the Ethernet port(s) in the port group.

Examples

Enable jumbo frames to pass through all the Ethernet ports in the manual port group named **group1**.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1] group-member GigabitEthernet 1/0/1
[Sysname-port-group-manual-group1] jumboframe enable
```

Enable jumbo frames to pass through GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] jumboframe enable
```

link-delay

Syntax

link-delay *delay-time*

undo link-delay

View

Ethernet port view

Default Level

2: System level

Parameters

delay-time: Up/down suppression time for the physical connection of an Ethernet port (in seconds). in the range 2 to 10.

Description

Use the **link-delay** command to configure the suppression time of physical-link-state changes on an Ethernet port.

Use the **undo link-delay** command to restore the default suppression time.

By default, the physical-link-state change suppression time is not configured.

Examples

Set the up/down suppression time of the physical connection of an Ethernet port to 8 seconds.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] link-delay 8
```

loopback

Syntax

loopback { **external** | **internal** }

undo loopback

View

Ethernet port view

Default Level

2: System level

Parameters

external: Enables external loopback testing on an Ethernet port.

internal: Enables internal loopback testing on an Ethernet port.

Description

Use the **loopback** command to enable Ethernet port loopback testing.

Use the **undo loopback** command to disable Ethernet port loopback testing.

By default, Ethernet port loopback testing is disabled.

Note

- Ethernet port loopback testing should be enabled while testing certain functionalities, such as during the initial identification of any network failure.
- While enabled, Ethernet port loopback testing will work in full-duplex mode. The interface will return to its original state upon completion of the loopback testing.

Examples

Enable loopback testing on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback internal
```

loopback-detection control enable

Syntax

loopback-detection control enable

undo loopback-detection control enable

View

Ethernet port view

Default Level

2: System level

Parameters

None

Description

Use the **loopback-detection control enable** command to enable loopback detection for a Trunk port or Hybrid port.

Use the **undo loopback-detection control enable** command to restore the default.

By default, loopback detection for a Trunk port or Hybrid port is disabled.

- When the loopback detection is enabled, if a port has been detected with loopback, it will be shut down. A Trap message will be sent to the terminal and the corresponding MAC address forwarding entries will be deleted.
- When the loopback detection is disabled, if a port has been detected with loopback, a Trap message will be sent to the terminal. The port is still working properly.

Note that this command is inapplicable to an Access port as its loopback detection is enabled by default.

Examples

Enable loopback detection for the trunk port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] loopback-detection enable
[Sysname-GigabitEthernet1/0/1] loopback-detection control enable
```

loopback-detection enable

Syntax

loopback-detection enable

undo loopback-detection enable

View

System view, Ethernet port view

Default Level

2: System level

Parameters

None

Description

Use the **loopback-detection enable** command to enable loopback detection globally or on a specified port.

Use the **undo loopback-detection enable** command to disable loopback detection globally or on a specified port.

By default, loopback detection is disabled for an Access, Trunk, or Hybrid port.

- If an Access port has been detected with loopback, it will be shut down. A Trap message will be sent to the terminal and the corresponding MAC address.
- If a Trunk port or Hybrid port has been detected with loopback, a Trunk message will be sent to the terminal. They will be shut down if the loopback testing function is enabled on them. In addition, a Trap message will be sent to the terminal and the corresponding MAC address forwarding entries will be deleted.

Related commands: **loopback-detection control enable**.

 **Caution**

- Loopback detection on a given port is enabled only after the **loopback-detection enable** command has been configured in both system view and interface view of the port.
- Loopback detection on all ports will be disabled after the configuration of the **undo loopback-detection enable** command in system view.

Examples

Enable loopback detection on the interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback-detection enable
```

loopback-detection interval-time

Syntax

loopback-detection interval-time *time*

undo loopback-detection interval-time

View

System view

Default Level

2: System level

Parameters

time: Time interval for performing port loopback detection, in the range 5 to 300 (in seconds).

Description

Use the **loopback-detection interval-time** command to configure time interval for performing port loopback detection.

Use the **undo loopback-detection interval-time** command to restore the default time interval for port loopback detection, which is 30 seconds.

Related commands: **display loopback-detection**.

Examples

Set the time interval for performing port loopback detection to 10 seconds.

```
<Sysname> system-view
[Sysname] loopback-detection interval-time 10
```

loopback-detection per-vlan enable

Syntax

loopback-detection per-vlan enable

undo loopback-detection per-vlan enable

View

Ethernet port view

Default Level

2: System level

Parameters

None

Description

Use the **loopback-detection per-vlan enable** command to enable loopback detection in all VLANs with Trunk ports or Hybrid ports.

Use the **undo loopback-detection per-vlan enable** command to enable loopback detection in the default VLAN with Trunk ports or Hybrid ports.

By default, loopback detection is only enabled in the default VLAN(s) with Trunk ports or Hybrid ports.

Note that the **loopback-detection per-vlan enable** command is not applicable to Access ports.

Examples

Enable loopback detection in all the VLANs to which the Hybrid port GigabitEthernet 1/1 belongs.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] loopback-detection enable
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] loopback-detection per-vlan enable
```

mdi

Syntax

mdi { **across** | **auto** | **normal** }

undo mdi

View

Ethernet port view

Default Level

2: System level

Parameters

across: Specifies the MDI mode as **across**.

auto: Specifies the MDI mode as **auto**.

normal: Specifies the MDI mode as **normal**.

Description

Use the **mdi** command to configure the MDI mode for an Ethernet port.

Use the **undo mdi** command to restore the system default.

By default, the MDI mode of an Ethernet port is **auto**, that is, the Ethernet port determines the physical pin roles (transmit or receive) through negotiation.

Note

The command is not applicable to optical interfaces of SFP ports or 10-Gigabit Ethernet ports.

Examples

Set the MDI mode of GigabitEthernet 1/0/1 to **across**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mdi across
```

multicast-suppression

Syntax

multicast-suppression { *ratio* | **pps** *max-pps* }

undo multicast-suppression

View

Ethernet port view, port group view

Default Level

2: System level

Parameters

ratio: Maximum percentage of multicast traffic to the total transmission capability of an Ethernet port, in the range 1 to 100. The smaller the ratio is, the less multicast traffic is allowed to pass through the interface.

pps *max-pps*: Specifies the maximum number of multicast packets allowed on an Ethernet port per second (in pps, representing packets per second).

- For a Gigabit port, the value range is 1 to 1488100.
- For a 10-Gigabit port, the value range is 1 to 14881000.

Note that:

- When a suppression granularity larger than 1 is specified on the device, the value of the **pps** keyword should be no smaller than and an integral multiple of the granularity. The multicast suppression threshold value configured through this keyword on an Ethernet port may not be the one that actually takes effect. To display the actual multicast suppression threshold value on an Ethernet port, you can use the **display interface** command.
- When no suppression granularity is specified or the suppression granularity is set to 1, the value of the **pps** keyword should be no smaller than 1, and the multicast suppression threshold value is the one that actually takes effect on the Ethernet port.

Description

Use the **multicast-suppression** command to configure multicast storm suppression ratio on an interface.

Use the **undo multicast-suppression** command to restore the default multicast suppression ratio.

By default, all multicast traffic is allowed to go through an Ethernet port, that is, multicast traffic is not suppressed.

If you execute this command in Ethernet port view, the configurations take effect only on the current interface. If you execute this command in port-group view, the configurations take effect on all ports in the port group.

Note that when multicast traffic exceeds the maximum value configured, the system will discard the extra packets so that the multicast traffic ratio can drop below the limit to ensure that the network functions properly.

Note

- If you set different suppression ratios in Ethernet port view or port-group view for multiple times, the latest configuration takes effect.
- Do not use the **multicast-suppression** command along with the **storm-constrain** command. Otherwise, the multicast storm suppression ratio configured may get invalid.

Examples

For Ethernet port GigabitEthernet 1/0/1, allow multicast traffic equivalent to 20% of the total transmission capability of GigabitEthernet 1/0/1 to pass.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] multicast-suppression 20
```

For all the ports of the manual port group **group1**, allow multicast traffic equivalent to 20% of the total transmission capability of each port to pass.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1] group-member GigabitEthernet 1/0/2
[Sysname-port-group-manual-group1] group-member GigabitEthernet 1/0/3
[Sysname-port-group-manual-group1] multicast-suppression 20
```

port-group manual

Syntax

port-group manual *port-group-name*

undo port-group manual *port-group-name*

View

System view

Default Level

2: System level

Parameters

port-group-name: Specifies name of a manual port group, a string of 1 to 32 characters.

Description

Use the **port-group manual** command to create a manual port group and enter manual port group view.

Use the **undo port-group manual** command to remove a manual port group.

By default, no manual port group is created.

Examples

Create a manual port group named **group1**.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1]
```

reset counters interface

Syntax

reset counters interface [*interface-type* [*interface-number*]]

View

User view

Default Level

2: System level

Parameters

interface-type: Interface type.

interface-number: Interface number.

Description

Use the **reset counters interface** command to clear the statistics of an interface.

Before sampling network traffic within a specific period of time on an interface, you need to clear the existing statistics.

- If neither interface type nor interface number is specified, this command clears the statistics of all the interfaces.
- If only the interface type is specified, this command clears the statistics of the interfaces that are of the interface type specified.
- If both the interface type and interface number are specified, this command clears the statistics of the specified interface.

Examples

Clear the statistics of GigabitEthernet 1/0/1.

```
<Sysname> reset counters interface GigabitEthernet 1/0/1
```

reset packet-drop interface

Syntax

reset packet-drop interface [*interface-type* [*interface-number*]]

View

Any view

Default Level

2: System level

Parameters

interface-type: Type of a specified interface.

interface-number: Number of a specified interface.

Description

Use the **reset packet-drop interface** command to clear statistics of dropped packets on an interface or multiple interfaces. Sometimes when you want to collect the statistics of dropped packets on an interface, you need to clear the old statistics on the interface first.

- If you do not specify an interface type or interface number, this command clears statistics of dropped packets on all the interfaces on the device.
- If you specify an interface type only, this command clears statistics of dropped packets on the specified type of interfaces.
- If you specify both the interface type and interface number, this command clears statistics of dropped packets on the specified interface.

Examples

Clear statistics of dropped packets on GigabitEthernet 1/0/1.

```
<Sysname> reset packet-drop interface GigabitEthernet 1/0/1
```

Clear statistics of dropped packets on all interfaces.

```
<Sysname> reset packet-drop interface
```

shutdown

Syntax

shutdown

undo shutdown

View

Ethernet port view

Default Level

2: System level

Parameters

None

Description

Use the **shutdown** command to shut down an Ethernet port.

Use the **undo shutdown** command to bring up an Ethernet port.

By default, an Ethernet port is in the up state.

In certain circumstances, modification to the interface parameters does not immediately take effect, and therefore, you need to shut down the relative interface to make the modification work.

Note that in case of a Combo port, only one interface (either the optical port or the electrical port) is active at a time. That is, once the optical port is active (after you execute the **undo shutdown** command), the electrical port will be inactive automatically, and vice versa.

Examples

Shut down interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] shutdown
```

Bring up interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo shutdown
```

speed

Syntax

speed { **10** | **100** | **1000** | **auto** }

undo speed

View

Ethernet port view

Default Level

2: System level

Parameters

10: Specifies the interface rate as 10 Mbps. The optical interface of an SFP port does not support the **10** keyword.

100: Specifies the interface rate as 100 Mbps. The optical interface of an SFP port does not support the **100** keyword.

1000: Specifies the interface rate as 1,000 Mbps.

auto: Specifies to determine the interface rate through auto-negotiation.

Description

Use the **speed** command to configure Ethernet port data rate.

Use the **undo speed** command to restore Ethernet port data rate.

Note that:

- On the electrical interface of an Ethernet port, the purpose of using the **speed** command to set the data transmission rate is to make it consistent with that of the peer.
- On an SFP port, the purpose of using the **speed** command to set the data transmission rate is to make it consistent with that of the pluggable optical module.

Related commands: **duplex**, **speed auto**.

 **Note**

10-Gigabit Ethernet ports do not support this command.

Examples

Configure the interface rate as 100 Mbps for interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] speed 100
```

speed auto

Syntax

speed auto [**10** | **100** | **1000**] *

undo speed

View

Ethernet port view

Default Level

2: System level

Parameters

10: Specifies the interface auto-negotiation rate as 10 Mbps.

100: Specifies the interface auto-negotiation rate as 100 Mbps.

1000: Specifies the interface auto-negotiation rate as 1000 Mbps..

Description

Use the **speed auto** command to configure the auto-negotiation rate range of the current Ethernet port.

Use the **undo speed** command to restore the default.

The default value of the command varies with your device models.

If you repeatedly use the **speed** command and the **speed auto** command to configure the rate of an interface, only the latest configuration takes effect. For example, if you configure **speed 100** after configuring **speed auto 100 1000** on an interface, the rate is 100 Mbps by force, with no negotiation performed between the interface and the peer end; if you configure **speed auto 100 1000** after configuring **speed 100** on the interface, the rate through negotiation can be either 100 Mbps or 1000 Mbps only.

Note that:

- If the auto negotiation rate range specified on the local port and that on the peer do not overlap, for example, 10 Mbps and 100 Mbps are specified on one end while 1000 Mbps is specified on the other, the auto negotiation of interface rate will fail.
- If the auto negotiation rate range specified on the local port and that on the peer overlap, for example, 10 Mbps and 100 Mbps are specified on one end while 100 Mbps and 1000 Mbps are specified on the other, the result of the interface rate auto negotiation is the overlapped part, that is, 100 Mbps in the example.

- If the auto negotiation rate range specified on the local port and that on the peer are the same, for example, 100 Mbps and 1000 Mbps are specified on both ends, the result of the interface rate auto negotiation is the larger value, that is, 1000 Mbps in the example.

 **Note**

- This function is available for auto-negotiation-capable Gigabit Layer-2 Ethernet electrical ports only..
- If you repeatedly use the **speed** and the **speed auto** commands to configure the transmission rate on an port, only the latest configuration takes effect.

Examples

Set the auto-negotiation rate of interface GigabitEthernet 1/0/1 to 10 Mbps or 1000 Mbps.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] speed auto 10 1000
```

storm-constrain

Syntax

storm-constrain { **broadcast** | **multicast** } { **pps** | **kbps** | **ratio** } *max-values min-values*

undo storm-constrain { **all** | **broadcast** | **multicast** }

View

Ethernet port view

Default Level

2: System level

Parameters

all: Disables the storm constrain function for all types of packets (that is, multicast packets, and broadcast packets).

broadcast: Enables/Disables the storm constrain function for broadcast packets.

multicast: Enables/Disables the storm constrain function for multicast packets.

pps: Specifies the storm constrain threshold in terms of number of packets.

kbps: Specifies the storm constrain threshold in terms of number of kilobytes.

ratio: Specifies the storm constrain threshold in terms of percentages of the received packets to the whole transmission capacity.

max-values: Upper threshold to be set, in pps, kbps, or percentages.

When the threshold is set in pps:

- For a Gigabit port, the value range is 1 to 1488100.

- For a 10-Gigabit port, the value range is 1 to 14881000.

When the threshold is set in kbps:

- For a Gigabit port, the value range is 1 to 1000000.
- For a 10-Gigabit port, the value range is 1 to 10000000.

When the threshold is set in percentages, that is, keyword **ratio** is used, the value range is 1 to 100.

min-values: Lower threshold to be set, in pps, kbps, or percentages.

- For lower threshold to be set, in pps, this value ranges from 1 to *max-values*.
- For lower threshold to be set, in kbps, this value ranges from 1 to *max-values*.
- For lower threshold to be set, in percentages, this value ranges from 1 to *max-values*.

Description

Use the **storm-constrain** command to enable the storm constrain function for specific type of packets and set the upper and lower thresholds.

Use the **undo storm-constrain** command to disable the storm constrain function for specific type of packets.

By default, the storm constrain function is not enabled.

Note

- Do not use the **storm-constrain** command along with the **unicast-suppression** command, the **multicast-suppression** command, or the **broadcast-suppression** command. Otherwise, traffics may be suppressed in an unpredictable way.
- An upper threshold cannot be less than the corresponding lower threshold. Besides, do not configure the two thresholds as the same value.

Examples

Enable the storm constrain function for broadcast packets on `GigabitEthernet` 1/0/1, setting the upper and lower threshold to 2000 kbps and 1500 kbps.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain broadcast kbps 2000 1500
```

Enable the storm constrain function for multicast packets on GigabitEthernet1/0/3 in terms of percentages of the received multicast packets to the port's total transmission capacity, setting the upper and lower threshold to 80% and 15%.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] storm-constrain multicast ratio 80 15
```

storm-constrain control

Syntax

storm-constrain control { **block** | **shutdown** }

undo storm-constrain control

View

Ethernet port view

Default Level

2: System level

Parameters

block: Blocks the traffic of a specific type on a port when the traffic detected exceeds the upper threshold.

shutdown: Shuts down a port when a type of traffic exceeds the corresponding upper threshold. A port shut down by the storm constrain function stops forwarding all types of packets.

Description

Use the **storm-constrain control** command to set the action to be taken when a type of traffic exceeds the corresponding upper threshold.

Use the **undo storm-constrain control** command to restore the default.

By default, no action is taken when a type of traffic exceeds the corresponding threshold.

Examples

Configure to block interface GigabitEthernet 1/0/1 when a type of traffic reaching it exceeds the corresponding upper threshold.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain control block
```

storm-constrain enable log

Syntax

storm-constrain enable log

undo storm-constrain enable log

View

Ethernet port view

Default Level

2: System level

Parameters

None

Description

Use the **storm-constrain enable log** command to enable log sending. With log sending enabled, the system sends log when traffic reaching a port exceeds the corresponding threshold or the traffic drops down below the lower threshold after exceeding the upper threshold.

Use the **undo storm-constrain enable log** command to disable log sending.

By default, log sending is enabled.

Examples

Disable log sending for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo storm-constrain enable log
```

storm-constrain enable trap

Syntax

storm-constrain enable trap

undo storm-constrain enable trap

View

Ethernet port view

Default Level

2: System level

Parameters

None

Description

Use the **storm-constrain enable trap** command to enable trap message sending. With trap message sending enabled, the system sends trap messages when traffic reaching a port exceeds the corresponding threshold or the traffic drops down below the lower threshold after exceeding the upper threshold.

Use the **undo storm-constrain enable trap** command to disable trap message sending.

By default, trap message sending is enabled.

Examples

Disable trap message sending for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo storm-constrain enable trap
```

storm-constrain interval

Syntax

storm-constrain interval *seconds*

undo storm-constrain interval

View

System view

Default Level

2: System level

Parameters

seconds: Interval for generating traffic statistics, in the range 1 to 300 (in seconds).

Description

Use the **storm-constrain interval** command to set the interval for generating traffic statistics.

Use the **undo storm-constrain interval** command to restore the default.

By default, the interval for generating traffic statistics is 10 seconds.

Note

- The interval set by the **storm-constrain interval** command is specifically for the storm constrain function. It is different form that set by the **flow-interval** command.
- For network stability consideration, configure the interval for generating traffic statistics to a value that is not shorter than the default.

Examples

Set the interval for generating traffic statistics to 60 seconds.

```
<Sysname> system-view
[Sysname] storm-constrain interval 60
```

unicast-suppression

Syntax

unicast-suppression { *ratio* | **pps** *max-pps* }

undo unicast-suppression

View

Ethernet port view, port group view

Default Level

2: System level

Parameters

ratio: Maximum percentage of unicast traffic to the total transmission capability of an Ethernet port, in the range of 1 to 100. The smaller the ratio is, the less unicast traffic is allowed through the interface.

pps *max-pps*: Specifies the maximum number of unknown unicast packets passing through an Ethernet port per second (in pps, representing packets per second).

- For a Gigabit port, the value range is 1 to 1488100;
- For a 10-Gigabit port, the value range is 1 to 14881000.

Note that:

- When a suppression granularity larger than 1 is specified on the device, the value of the **pps** keyword should be no smaller than and an integral multiple of the granularity. The unicast suppression threshold value configured through this keyword on an Ethernet port may not be the one that actually takes effect. To display the actual unicast suppression threshold value on an Ethernet port, you can use the **display interface** command.
- When no suppression granularity is specified or the suppression granularity is set to 1, the value of the **pps** keyword should be no smaller than 1, and the unicast suppression threshold value is the one that actually takes effect on the Ethernet port.

Description

Use the **unicast-suppression** command to configure a unicast storm suppression ratio.

Use the **undo unicast-suppression** command to restore the default unicast suppression ratio.

By default, all unicast traffic is allowed to go through an Ethernet port, that is, unicast traffic is not suppressed.

If you execute this command in Ethernet port view, the configurations take effect only on the current interface. If you execute this command in port-group view, the configurations take effect on all ports in the port group

Note that when unicast traffic exceeds the maximum value configured, the system will discard the extra packets so that the unknown unicast traffic ratio can drop below the limit to ensure that the network functions properly.

Note

- If you set different suppression ratios in Ethernet port view or port-group view repeatedly, the latest configuration takes effect.
- Do not use the **unicast-suppression** command along with the **storm-constrain** command. Otherwise, the unicast storm suppression ratio configured may get invalid.

Examples

For Ethernet port GigabitEthernet 1/0/1, allow unknown unicast traffic equivalent to 20% of the total transmission capability of the interface to pass and suppress the excessive unknown unicast packets.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] unicast-suppression 20
```

For all the ports of the manual port group **group1**, allow unknown unicast traffic equivalent to 20% of the total transmission capability of each port to pass and suppress excessive unknown unicast packets.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1] group-member GigabitEthernet 1/0/5
[Sysname-port-group-manual-group1] group-member GigabitEthernet 1/0/6
[Sysname-port-group-manual-group1] unicast-suppression 20
```

virtual-cable-test

Syntax

virtual-cable-test

View

Ethernet port view

Default Level

2: System level

Parameters

None

Description

Use the **virtual-cable-test** command to test the cable connected to the Ethernet port once and to display the testing result. The tested items include:

Note that:

- When the cable is functioning properly, the cable length in the test result represents the total cable length;
- When the cable is not functioning properly, the cable length in the test result represents the length from the current interface to the failed position.

 **Note**

- 10-Gigabit ports and optical interfaces of SFP ports do not support this command.
- A link in the up state goes down and then up automatically if you execute this command on one of the Ethernet ports forming the link.
- The test result is for your information only. The maximum error in the tested cable length is 5 m. A hyphen “-” indicates that the corresponding test item is not supported.

Examples

Enable the virtual cable test for the interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] virtual-cable-test
Cable status: normal, 1 metres
Pair Impedance mismatch: -
Pair skew: - ns
Pair swap: -
Pair polarity: -
Insertion loss: - db
Return loss: - db
Near-end crosstalk: - db
```

1 Link Aggregation Configuration Commands

Link Aggregation Configuration Commands

description

Syntax

description *text*

undo description

View

Layer-2 aggregate interface view

Default Level

2: System level

Parameters

text: Description of an Ethernet interface, a string of 1 to 80 characters. Currently, the device supports the following types of characters or symbols: standard English characters (numbers and case-sensitive letters), special English characters, spaces, and other characters or symbols that conform to the Unicode standard.

Note

- A port description can be the mixture of English characters and other Unicode characters. The mixed description cannot exceed the specified length.
- To use a type of Unicode characters or symbols in a port description, you need to install the corresponding Input Method Editor (IME) and log in to the device through remote login software that supports this character type.
- Each Unicode character or symbol (non-English characters) takes the space of two regular characters. When the length of a description string reaches or exceeds the maximum line width on the terminal software, the software starts a new line, possibly breaking a Unicode character into two. As a result, garbled characters may be displayed at the end of a line.

Description

Use the **description** command to set the description of the current interface.

Use the **undo description** command to restore the default.

By default, the description of an interface is *interface-name* **Interface**, such as **Bridge-Aggregation1 Interface**.

Examples

Set the description of interface Bridge-aggregation 1 to **link-aggregation interface**.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] description link-aggregation interface
```

display lacp system-id

Syntax

display lacp system-id

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display lacp system-id** command to display the system ID of the local system (that is, the actor).

The system ID comprises the system LACP priority and the system MAC address.

You can use the **lacp system-priority** command to change the LACP priority of the local system. When you do that, the LACP priority value you specify in the command is in decimal format. However, it is displayed as a hexadecimal value with the **display lacp system-id** command.

Related commands: **lacp system-priority**.

Examples

Display the local system ID.

```
<Sysname> display lacp system-id
 Actor System ID: 0x8000, 00e0-fc00-0100
```

Table 1-1 display lacp system-id command output description

Field	Description
Actor System ID: 0x8000, 00e0-fc00-0100	The local system ID, which comprises the LACP system priority (0x8000 in this sample output) and the system MAC address (00e0-fc00-0100 in this sample output).

display link-aggregation load-sharing mode

Syntax

display link-aggregation load-sharing mode [**interface** [**bridge-aggregation** *interface-number*]]

View

Any view

Default Level

1: Monitor level

Parameters

bridge-aggregation: Displays the load sharing mode of the aggregation group corresponding to the specified Layer 2 aggregate interface.

interface-number: Specifies the number of an existing aggregate interface.

Description

Use the **display link-aggregation load-sharing mode** command to display load sharing mode for link aggregation groups.

To display the global link aggregation load sharing mode, perform the command without the **interface** keyword.

To display the load sharing mode of the aggregation group corresponding to each aggregate interface, perform the command with the **interface** keyword but do not specify a particular interface.

To display the load sharing mode of a particular aggregation group, perform the command with the aggregate interface specified.

Examples

Display the default global link aggregation load sharing mode.

```
<Sysname> display link-aggregation load-sharing mode

Link-Aggregation Load-Sharing Mode:
Layer 2 traffic: destination-mac address, source-mac address
Layer 3 traffic: destination-ip address,  source-ip address
```

Display the configured global link aggregation load sharing mode.

```
<Sysname> display link-aggregation load-sharing mode

Link-Aggregation Load-Sharing Mode:
  destination-mac address, source-mac address
```

Display the default link aggregation load sharing mode of the aggregation group corresponding to Layer 2 aggregate interface Bridge-Aggregation 10.

```
<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 10

Bridge-Aggregation1 Load-Sharing Mode:
Layer 2 traffic: destination-mac address, source-mac address
Layer 3 traffic: destination-ip address,  source-ip address
```

Display the configured link aggregation load sharing mode of the aggregation group corresponding to Layer 2 aggregate interface Bridge-Aggregation 10.

```
<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 10
```

```
Bridge-Aggregation1 Load-Sharing Mode:
  destination-mac address, source-mac address
```

Display the link aggregation load sharing mode of each aggregation group.

```
<Sysname> display link-aggregation load-sharing mode interface

Bridge-Aggregation10 Load-Sharing Mode:
  destination-ip address,  source-ip address

Bridge-Aggregation20 Load-Sharing Mode:
Layer 2 traffic: destination-mac address, source-mac address
Layer 3 traffic: destination-ip address,  source-ip address
```

Table 1-2 display link-aggregation load-sharing mode command output description

Field	Description
Link-Aggregation Load-Sharing Mode	Displays the global link aggregation load sharing mode. • By default, the link aggregation load sharing modes for Layer-2 traffic, and Layer-3 traffic displayed. • If you have configured a global load sharing mode, the configured mode is displayed.
Layer 2 traffic: destination-mac address, source-mac address	The default load sharing mode for Layer-2 traffic. In this sample output, it is based on source MAC address and destination MAC address.
Layer 3 traffic: destination-ip address, source-ip address	The default load sharing mode for Layer-3 traffic. In this sample output, it is based on source IP address and destination IP address.
destination-mac address, source-mac address	The user-configured link aggregation load sharing mode. In this sample output, it is based on source MAC address and destination MAC address.

display link-aggregation member-port

Syntax

display link-aggregation member-port [*interface-type interface-number* [**to** *interface-type interface-number*]]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Port type and port number.

to: Specifies an interface range in the form of *interface-type interface-number* **to** *interface-type interface-number*, where the start interface number must be smaller than the end interface number. Note that both the start interface and the end interface are inclusive.

Description

Use the **display link-aggregation member-port** command to display the detailed link aggregation information of the specified interface(s) or all interfaces if no interface is specified.

For an interface in a static aggregation group, only its port number and operational key are displayed, because it is not aware of the information of the partner.

Examples

Display the detailed link aggregation information of GigabitEthernet 1/0/1, which is in a static aggregation group.

```
<Sysname> display link-aggregation member-port GigabitEthernet 1/0/1

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
      D -- Synchronization, E -- Collecting, F -- Distributing,
      G -- Defaulted, H -- Expired

GigabitEthernet1/0/1:
Aggregation Interface: Bridge-Aggregation1
Port Number: 1
Oper-Key: 1
```

Display the detailed link aggregation information of GigabitEthernet 1/0/2, which is in a dynamic aggregation group.

```
<Sysname> display link-aggregation member-port GigabitEthernet 1/0/2

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
      D -- Synchronization, E -- Collecting, F -- Distributing,
      G -- Defaulted, H -- Expired

GigabitEthernet1/0/2:
Aggregation Interface: Bridge-Aggregation10
Local:
   Port Number: 2
   Port Priority: 32768
   Oper-Key: 2
   Flag: {ACDEF}
Remote:
   System ID: 0x8000, 000f-e267-6c6a
   Port Number: 26
   Port Priority: 32768
   Oper-Key: 2
   Flag: {ACDEF}
Received LACP Packets: 5 packet(s)
Illegal: 0 packet(s)
Sent LACP Packets: 7 packet(s)
```

Table 1-3 display link-aggregation member-port command output description

Field	Description
Flags	One-octet LACP state flags field. From the least to the most significant bit, they are represented by A through H as follows: • A indicates whether LACP is enabled. 1 for enabled and 0 for disabled. • B indicates the timeout control value. 1 for short timeout, and 0 for long timeout. • C indicates whether the link is considered as aggregatable by the sending system. 1 for true, and 0 for false. • D indicates whether the link is considered as synchronized by the sending system. 1 for true, and 0 for false. • E indicates whether the sending system considers that collection of incoming frames is enabled on the link. 1 for true and 0 for false. • F indicates whether the sending system considers that distribution of outgoing frames is enabled on the link. 1 for true and 0 for false. • G indicates whether the receive state machine of the sending system is using default operational partner information. 1 for true and 0 for false. • H indicates whether the receive state machine of the sending system is in the expired state. 1 for true and 0 for false. If a flag bit is set to 1, the corresponding English letter that otherwise is not output is displayed.
Aggregation Interface	Aggregate interface to which the port belongs
Local: Port Number Port Priority Oper-key Flag	Information about the local end: • Port Number: Number of the port. • Port Priority: LACP priority of the port. • Oper-key: Operational key • Flag: LACP protocol state flag.
Remote: System ID Port Number Port Priority Oper-key Flag	Information about the remote end: • System ID: System ID of the remote end, comprising the system LACP priority and the system MAC address. • Port Number: Number of the port. • Port Priority: LACP priority of the port. • Oper-key: Operational key • Flag: LACP protocol state flag.
Received LACP Packets	Number of LACP packets received
Illegal	Number of illegal packets
Sent LACP Packets	Number of LACP packets sent

display link-aggregation summary

Syntax

display link-aggregation summary

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display link-aggregation summary** command to display the summary information of all aggregation groups.

You may find out that information about the remote system for a static link aggregation group is either replaced by **none** or not displayed at all. This is normal because this type of aggregation group is not aware of its partner.

Examples

Display the summary information of all aggregation groups.

```
<Sysname> display link-aggregation summary

Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e267-6c6a

AGG        AGG      Partner ID             Select Unselect   Share
Interface   Mode                           Ports  Ports     Type
--------------------------------------------------------------------------------
BAGG1      S        none                   1      0         Shar
BAGG10     D        0x8000, 000f-e267-57ad   2      0         Shar
```

Table 1-4 display link-aggregation summary command output description

Field	Description
Aggregation Interface Type	Aggregate interface type: • BAGG for a Layer-2 aggregate interface • RAGG for a Layer-3 aggregate interface
Aggregation Mode	Aggregation group type: • S for static link aggregation • D for dynamic aggregation
Loadsharing Type	Loadsharing type: • Shar for load sharing • NonS for non-load sharing
Actor System ID	Local system ID, which comprises the system LACP priority and the system MAC address
AGG Interface	Abbreviated name of the aggregate interface
AGG Mode	Aggregation group type
Partner ID	System ID of the partner, which comprises the system LACP priority and the system MAC address

Field	Description
Select Ports	The number of selected ports
Unselect Ports	The number of unselected ports
Share Type	Load sharing type

display link-aggregation verbose

Syntax

display link-aggregation verbose [**bridge-aggregation** [*interface-number*]]

View

Any view

Default Level

1: Monitor level

Parameters

bridge-aggregation: Displays detailed information about the Layer-2 aggregate groups corresponding to Layer-2 aggregate interfaces.

interface-number: Aggregate interface number. Note that the aggregate interface you specify must already exist.

Description

Use the **display link-aggregation verbose** command to display detailed information about the aggregation groups corresponding to the aggregate interfaces.

To display the information of a specific Layer-2 aggregate group, use the **display link-aggregation verbose bridge-aggregation** *interface-number* command.

To display the information of all Layer-2 aggregate groups, use the **display link-aggregation verbose bridge-aggregation** command.

To display the information of all aggregate groups, use the **display link-aggregation verbose** command.

Examples

Display the detailed information of the aggregation group corresponding to Layer-2 aggregate interface **Bridge-aggregation 10**.

```
<Sysname> display link-aggregation verbose bridge-aggregation 10

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected,  U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation10
```

```
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port           Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/6          S      32768    2        {ACDEF}
  GE1/0/12         S      32768    2        {ACDEF}
Remote:
  Actor          Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/6          32      32768     2        0x8000, 000f-e267-57ad {ACDEF}
  GE1/0/12         26      32768     2        0x8000, 000f-e267-57ad {ACDEF}
```

Table 1-5 display link-aggregation verbose command output description

Field	Description
Loadsharing Type	Loadsharing type: • Shar for load sharing • NonS for non-load sharing
Port Status	Port state: Selected or unselected.
Flags	One-octet LACP state flags field. From the least to the most significant bit, they are represented by A through H as follows: • A indicates whether LACP is enabled. 1 for enabled and 0 for disabled. • B indicates the timeout control value. 1 for short timeout, and 0 for long timeout. • C indicates whether the link is considered as aggregatable by the sending system. 1 for true, and 0 for false. • D indicates whether the link is considered as synchronized by the sending system. 1 for true, and 0 for false. • E indicates whether the sending system considers that collection of incoming frames is enabled on the link. 1 for true and 0 for false. • F indicates whether the sending system considers that distribution of outgoing frames is enabled on the link. 1 for true and 0 for false. • G indicates whether the receive state machine of the sending system is using default operational partner information. 1 for true and 0 for false. • H indicates whether the receive state machine of the sending system is in the expired state. 1 for true and 0 for false. If a flag bit is set to 1, the corresponding English letter that otherwise is not output is displayed.
Aggregation Interface	Name of the aggregate interface
Aggregation Mode	Type of the aggregation group: Static for static aggregation, and Dynamic for dynamic aggregation.
System ID	Local system ID, which comprises the system LACP priority and the system MAC address.
Local: Port Status Priority Oper-Key Flag	Other information of the local end, including the member ports, port state, port LACP priority, operational key, and LACP protocol state flags.

Field	Description
Remote: Actor Partner Priority Oper-Key SystemID Flag	Detailed information about the remote end, including the corresponding local port, port ID, port LACP priority, operational key, system ID, and LACP protocol state flags

enable snmp trap updown

Syntax

enable snmp trap updown

undo enable snmp trap updown

View

Layer-2 aggregate interface view

Default Level

2: System level

Parameters

None

Description

Use the **enable snmp trap updown** command to enable linkUp/linkDown trap generation for the current aggregate interface.

Use the **undo enable snmp trap updown** command to disable linkUp/linkDown trap generation for the current aggregate interface.

By default, linkUp/linkDown trap generation is enabled for an aggregate interface.

Note that for an aggregate interface to generate linkUp/linkDown traps when its link state changes, you must also enable linkUp/linkDown trap generation globally with the **snmp-agent trap enable** [**standard** [**linkdown** | **linkup**] *] command.

Refer to *SNMP Commands* in the *System Volume* for information about the **snmp-agent trap enable** command.

Examples

Enable linkUp/linkDown trap generation on interface **Bridge-aggregation 1**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] enable snmp trap updown
```

interface bridge-aggregation

Syntax

interface bridge-aggregation *interface-number*

undo interface bridge-aggregation *interface-number*

View

System view

Default Level

2: System level

Parameters

interface-number: Layer-2 aggregate interface number. The value range is 1 to 128

Description

Use the **interface bridge-aggregation** command to create a Layer-2 aggregate interface and enter the Layer-2 aggregate interface view.

Use the **undo interface bridge-aggregation** command to remove a Layer-2 aggregate interface.

Upon creation of a Layer-2 aggregate interface, a Layer-2 aggregation group numbered the same is created automatically. Removing the Layer-2 aggregate interface also removes the Layer-2 aggregation group. At the same time, the member ports of the aggregation group, if any, leave the aggregation group.

Examples

Create Layer-2 aggregate interface **Bridge-aggregation 1**.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1]
```

lacp port-priority

Syntax

lacp port-priority *port-priority*

undo lacp port-priority

View

Ethernet interface view

Default Level

2: System level

Parameters

port-priority: LACP port priority, in the range of 0 to 65535.

Description

Use the **lacp port-priority** command to set the LACP priority of a port.

Use the **undo lacp port-priority** command to restore the default.

The default LACP priority of a port is 32768.

Examples

Set the LACP priority of GigabitEthernet 1/0/1 to 64.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lacp port-priority 64
```

lacp system-priority

Syntax

lacp system-priority *system-priority*

undo lacp system-priority

View

System view

Default Level

2: System level

Parameters

system-priority: LACP priority of the local system, in the range of 0 to 65535.

Description

Use the **lacp system-priority** command to set the LACP priority of the local system.

Use the **undo lacp system-priority** command to restore the default.

By default, the system LACP priority is 32768.

Examples

Set the system LACP priority to 64.

```
<Sysname> system-view
[Sysname] lacp system-priority 64
```

link-aggregation load-sharing mode (system view)

Syntax

link-aggregation load-sharing mode { **destination-ip** | **destination-mac** | **destination-port** | **ingress-port** | **source-ip** | **source-mac** | **source-port** } *

undo link-aggregation load-sharing mode

View

System view

Default Level

2: System level

Parameters

destination-ip: Specifies to perform load sharing in link aggregation groups based on destination IP address.

destination-mac: Specifies to perform load sharing in load-sharing link aggregation groups based on destination MAC address.

destination-port: Specifies to perform load sharing in load-sharing link aggregation groups based on destination port.

ingress-port: Specifies to perform load sharing in load-sharing link aggregation groups based on ingress port.

source-ip: Specifies to perform load sharing in load-sharing link aggregation groups based on source IP address.

source-mac: Specifies to perform load sharing in load-sharing link aggregation groups based on source MAC address.

source-port: Specifies to perform load sharing in load-sharing link aggregation groups based on source port.

Description

Use the **link-aggregation load-sharing mode** command to configure the link aggregation load sharing mode.

Use the **undo link-aggregation load-sharing mode** command to restore the default.

By default, link aggregation load sharing for Layer-2 packets is performed based on source MAC addresses and destination MAC addresses, and that for Layer-3 packets is performed based on source IP addresses and destination IP addresses.

Note that:

- The load sharing mode you configured overwrites rather than adds to the old one, if any. Therefore, to change the load sharing mode from source mac based to source and destination mac based for example, you must configure the **link-aggregation load-sharing mode destination-mac source-mac** to overwrite the **link-aggregation load-sharing mode destination-mac** command rather than configure the **link-aggregation load-sharing mode source-mac** command.
- In case an unsupported load sharing mode is configured, you will be prompted of the error..

Examples

Configure the link aggregation load sharing mode as destination MAC-based.

```
<Sysname> system-view
[Sysname] link-aggregation load-sharing mode destination-mac
```

link-aggregation load-sharing mode (aggregate interface view)

Syntax

link-aggregation load-sharing mode { **destination-ip** | **destination-mac** | **source-ip** | **source-mac** | } *

undo link-aggregation load-sharing mode

View

Layer 2 aggregate interface view

Default Level

2: System level

Parameters

destination-ip: Specifies to perform load sharing in link aggregation groups based on destination IP address.

destination-mac: Specifies to perform load sharing in load-sharing link aggregation groups based on destination MAC address.

source-ip: Specifies to perform load sharing in load-sharing link aggregation groups based on source IP address.

source-mac: Specifies to perform load sharing in load-sharing link aggregation groups based on source MAC address.

Description

Use the **link-aggregation load-sharing mode** command to configure the aggregation group-specific link aggregation load sharing mode.

Use the **undo link-aggregation load-sharing mode** command to restore the default.

The global link aggregation load sharing mode is the default for all link aggregation groups.

Note that:

- The load sharing mode you configured overwrites rather than adds to the old one, if any. Therefore, to change the load sharing mode from source mac based to source and destination mac based for example, you must configure the **link-aggregation load-sharing mode destination-mac source-mac** to overwrite the **link-aggregation load-sharing mode destination-mac** command rather than configure the **link-aggregation load-sharing mode source-mac** command.
- In case an unsupported load sharing mode is configured, you will be prompted of the error.

Examples

Configure the load sharing mode of the link aggregation group corresponding to Bridge-Aggregation 10 as destination MAC-based.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 10
[Sysname-Bridge-Aggregation10] link-aggregation load-sharing mode destination-mac
```

link-aggregation mode

Syntax

link-aggregation mode dynamic

undo link-aggregation mode

View

Layer-2 aggregate interface view

Default Level

2: System level

Parameters

None

Description

Use the **link-aggregation mode dynamic** command to configure an aggregation group to work in dynamic aggregation mode.

Use the **undo link-aggregation mode** command to restore the default.

By default, an aggregation group works in static aggregation mode.

If there is any member port in an aggregation group, you cannot modify the aggregation mode of the aggregation group.

Examples

Configure the aggregation group of **Bridge-aggregation 1** to work in dynamic aggregation mode.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic
```

port link-aggregation group

Syntax

port link-aggregation group *number*

undo port link-aggregation group

View

Ethernet interface view

Default Level

2: System level

Parameters

number: Aggregate group number. The value range is 1 to 128.

Description

Use the **port link-aggregation group** command to assign the current Ethernet interface to the specified aggregation group.

Use the **undo port link-aggregation group** command to remove the current Ethernet interface from the specified aggregation group.

Note that

- If the Ethernet interface is a Layer-2 interface, you must assign it to a Layer-2 aggregation group.
- An Ethernet interface can belong to only one aggregation group.

Examples

Assign GigabitEthernet 1/0/1 to aggregation group 22.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-aggregation group 22
```

reset counters interface

Syntax

reset counters interface [**bridge-aggregation** [*interface-number*]]

View

User view

Default Level

2: System level

Parameters

bridge-aggregation: Clears statistics for Layer 2 aggregate interfaces.

interface-number: Aggregate interface number. If the *interface-number* argument is not specified, this command clears statistics of all aggregate interfaces of the specified type.

Description

Use the **reset counters interface** command to clear the statistics of the specified aggregate interface or interfaces.

Before collecting statistics for a Layer 2 aggregate interface within a specific period, you need to clear the existing statistics of the interface.

Note that:

- If none of the keywords and argument is specified, this command clears the statistics of all interfaces in the system.
- If only the **bridge-aggregation** or **route-aggregation** keyword is specified, the command clears the statistics of all Layer 2 aggregate interfaces.
- If the **bridge-aggregation** *interface-number* or **route-aggregation** *interface-number* keyword and argument combination is specified, this command clears the statistics of the specified Layer 2 aggregate interface.

Examples

Clear the statistics of Layer 2 aggregate interface bridge-aggregation 1.

```
<Sysname> reset counters interface bridge-aggregation 1
```

reset lacp statistics

Syntax

reset lacp statistics [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]]

View

User view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Interface type and interface number.

to: Specifies an interface range in the form of *interface-type interface-number* **to** *interface-type interface-number*, where the start interface number must be smaller than the end interface number. Note that both the start interface and the end interface are inclusive.

Description

Use the **reset lacp statistics** command to clear the LACP statistics for the specified interface(s) or all interfaces if no interface is specified.

Related commands: **display link-aggregation member-port**.

Examples

Clear the LACP statistics for all Ethernet ports.

```
<Sysname> reset lacp statistics
```

shutdown

Syntax

shutdown

undo shutdown

View

Layer-2 aggregate interface view

Default Level

2: System level

Parameters

None

Description

Use the **shutdown** command to shut down the current aggregate interface/subinterface.

Use the **undo shutdown** command to bring up the current aggregate interface/subinterface.

By default, aggregate interfaces are enabled.

Examples

Shut down aggregate interface **Bridge-Aggregation 1**.

```
<Sysname> system-view
```

```
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] shutdown
```

2 Port Isolation Configuration Commands

Port Isolation Configuration Commands

display port-isolate group

Syntax

display port-isolate group

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display port-isolate group** command to display information about the default isolation group (isolation group 1).

Examples

On a single-isolation-group device, display information about the isolation group.

```
<Sysname> display port-isolate group
Port-isolate group information:
 Uplink port support: NO
 Group ID: 1
 Group members:
    GigabitEthernet1/0/1
```

Table 2-1 display port-isolate group command output description

Field	Description
Port-isolate group information	Display the information of a port-isolation group
Uplink port support	Indicates whether the uplink port is supported.
Group ID	Isolation group number
Group members	Isolated ports in the isolation group

port-isolate enable

Syntax

port-isolate enable

undo port-isolate enable

View

Ethernet interface view, Layer-2 aggregate interface view, port group view

Default Level

2: System level

Parameters

None

Description

Use the **port-isolate enable** command to add a port in Ethernet interface view or a group of ports in port group view to an isolation group as isolated ports.

Use the **undo port-isolate enable** command to remove the port or ports from the isolation group.

- In Ethernet interface view, the configuration applies to the current port.
- In port group view, the configuration applies to all ports in the port group.
- In Layer-2 aggregate interface view, the configuration applies to the Layer-2 aggregate interface and all its member ports. After you make the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For detailed information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

Examples

On a single-isolation-group device, assign ports GigabitEthernet 1/1 and GigabitEthernet 1/2 to the isolation group.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-isolate enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port-isolate enable
```

On a single-isolation-group device, assign all the ports within port group **aa** to the isolation group.

```
<Sysname> system-view
[Sysname] port-group manual aa
[Sysname-port-group-manual-aa] group-member GigabitEthernet 1/0/1
[Sysname-port-group-manual-aa] group-member GigabitEthernet 1/0/2
[Sysname-port-group-manual-aa] group-member GigabitEthernet 1/0/3
[Sysname-port-group-manual-aa] group-member GigabitEthernet 1/0/4
[Sysname-port-group-manual-aa] port-isolate enable
```

Assign Layer-2 aggregate interface **Bridge-aggregation 1** and its member ports to the isolation group on a single-isolation-group device.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-aggregation group 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port link-aggregation group 1
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port-isolate enable
```

3 MSTP Configuration Commands

MSTP Configuration Commands

active region-configuration

Syntax

active region-configuration

View

MST region view

Default Level

2: System level

Parameters

None

Description

Use the **active region-configuration** command to activate your MST region configuration.

Note that:

- The configuration of MST region–related parameters, especially the VLAN-to-instance mapping table, will cause MSTP to launch a new spanning tree calculation process, which may result in network topology instability. To reduce the possibility of topology instability caused by configuration, MSTP will not immediately launch a new spanning tree calculation process when processing MST region–related configurations; instead, such configurations will take effect only after you activate the MST region–related parameters using this command, or enable MSTP using the **stp enable** command in the case that MSTP is not enabled.
- Before running this command, you are recommended to use the **check region-configuration** command to check whether the MST region configurations to be activated are correct. You should run this command only if the result returns positive.

Related commands: **instance**, **region-name**, **revision-level**, **vlan-mapping modulo**, **check region-configuration**.

Examples

Map VLAN 2 to MSTI 1 and activate MST region configuration manually.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
[Sysname-mst-region] active region-configuration
```

bpdu-drop any

Syntax

bpdu-drop any

undo bpdu-drop any

View

Ethernet interface view, port group view, Layer-2 aggregate interface view

Default Level

2: System level

Parameters

None

Description

Use the **bpdu-drop any** command to enable BPDU dropping on the Ethernet port.

Use the **undo bpdu-drop any** command to disable BPDU dropping on the Ethernet port.

By default, BPDU dropping is disabled.

In a STP-enabled network, some users may send BPDU packets to the switch continuously in order to destroy the network. When a switch receives the BPDU packets, it will forward them to other switches. As a result, STP calculation is performed repeatedly, which may occupy too much CPU of the switches or cause errors in the protocol state of the BPDU packets.

In order to avoid this problem, you can enable BPDU dropping on Ethernet ports. Once the function is enabled on a port, the port will not receive or forward any BPDU packets. In this way, the switch is protected against the BPDU packet attack and the STP calculation correctness is ensured.

Examples

Enable BPDU dropping on GigabitEthernet 1/0/1.

```
<Sysname>system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bpdu-drop any
```

check region-configuration

Syntax

check region-configuration

View

MST region view

Default Level

2: System level

Parameters

None

Description

Use the **check region-configuration** command to view MST region configuration information not activated yet, including the region name, revision level, and VLAN-to-instance mapping settings.

Note that:

- Two or more MSTP-enabled devices belong to the same MST region only if they are configured to have the same format selector, MST region name, the same VLAN-to-instance mapping entries in the MST region and the same MST region revision level, and they are interconnected via a physical link.
- Before activating the configurations of an MST region, you are recommended to use this command to check whether the MST region configurations are correct. You should activate the MST region configurations only if the result returns positive.

Related commands: **instance**, **region-name**, **revision-level**, **vlan-mapping modulo**, **active region-configuration**.

Examples

View MST region configurations that are not yet activated.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] check region-configuration
Admin Configuration
   Format selector    :0
   Region name       :000fe26a58ed
   Revision level     :0

   Instance   Vlans Mapped
      0       1 to 9, 11 to 4094
     15       10
```

Table 3-1 check region-configuration command output description

Field	Description
Format selector	Format selector of the MST region, which defaults to 0 and is not configurable.
Region name	MST region name
Revision level	Revision level of the MST region
Instance Vlans Mapped	VLAN-to-instance mappings in the MST region

display stp

Syntax

display stp [**instance** *instance-id*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]

View

Any view

Default Level

1: Monitor level

Parameters

instance *instance-id*: Displays the status and statistics information of a particular MSTI. The minimum value of *instance-id* is 0, representing the common internal spanning tree (CIST), and the maximum value of *instance-id* is 32.

interface *interface-list*: Displays the MSTP status and statistics information on the ports specified by a port list, in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 ports or port ranges.

slot *slot-number*: Displays the spanning tree information of the specified IRF member device. The slot-number argument is the member number of the device in the IRF, which you can display with the **display irf** command. The value range for the slot-number argument depends on the number of members and numbering conditions in the current IRF. If no IRF exists, the slot-number argument is the current device number.

brief: Displays brief MSTP status and statistics information.

Description

Use the **display stp** command to view the MSTP status and statistics information.

Based on the MSTP status and statistics information, you can analyze and maintain the network topology or check whether MSTP is working normally.

Note that:

- If you do not specify any MSTI or port, this command will display the MSTP information of all MSTIs on all ports. The displayed information is sorted by MSTI ID and by port name in each MSTI.
- If you specify an MSTI but not a port, this command will display the MSTP information on all ports in that MSTI. The displayed information is sorted by port name.
- If you specify some ports but not an MSTI, this command will display the MSTP information of all MSTIs on the specified ports. The displayed information is sorted by MSTI ID, and by port name in each MSTI.
- If you specify both an MSTI ID and a port list, this command will display the MSTP information on the specified ports in the specified MSTI. The displayed information is sorted by port name.

The MSTP status information includes:

- CIST global parameters: Protocol work mode, device priority in the CIST (Priority), MAC address, hello time, max age, forward delay, maximum hops, common root of the CIST, external path cost from the device to the CIST common root, regional root, the internal path cost from the device to the regional root, CIST root port of the device, and status of the BPDU guard function (enabled or disabled).
- CIST port parameters: Port status, role, priority, path cost, designated bridge, designated port, edge port/non-edge port, whether connecting to a point-to-point link, maximum transmission rate (transmit limit), status of the root guard function (enabled or disabled), BPDU format, boundary port/non-boundary port, hello time, max age, forward delay, message age, remaining hops, and whether rapid state transition enabled for designated ports.

- MSTI global parameters: MSTI ID, bridge priority of the MSTI, regional root, internal path cost, MSTI root port, and master bridge.
- MSTI port parameters: Port status, role, priority, path cost, designated bridge, designated port, remaining hops, and whether rapid state transition enabled (for designated ports).

The statistics information includes:

- The number of TCN BPDUs, configuration BPDUs, RST BPDUs and MST BPDUs sent from each port
- The number of TCN BPDUs, configuration BPDUs, RST BPDUs, MST BPDUs and wrong BPDUs received on each port
- The number of BPDUs discarded on each port

Related commands: **reset stp**.

Examples

View the brief MSTP status and statistics information.

```
<Sysname> display stp instance 0 interface gigabitethernet 1/0/1 to gigabitethernet 1/0/4
brief
 MSTID     Port                    Role  STP State     Protection
   0       GigabitEthernet1/0/1      DESI  FORWARDING    NONE
   0       GigabitEthernet1/0/2      DESI  FORWARDING    NONE
   0       GigabitEthernet1/0/3      DESI  FORWARDING    NONE
   0       GigabitEthernet1/0/4      DESI  FORWARDING    NONE
```

Table 3-2 display stp brief command output description

Field	Description
MSTID	MSTI ID in the MST region
Port	Port name, corresponding to each MSTI
Role	Port role, which can be one of the following: • ALTE: The port is an alternate port • BACK: The port is a backup port • ROOT: The port is a root port • DESI: The port is a designated port • MAST: The port is a master port • DISA: The port is disabled
STP State	MSTP status on the port, which can be: • FORWARDING: The port learns MAC addresses and forwards user traffic • DISCARDING: The port does not learn MAC addresses or forward user traffic • LEARNING: The port learns MAC addresses but does not forward user traffic
Protection	Protection type on the port, which can be: • ROOT: Root guard • LOOP: Loop guard • BPDU: BPDU guard • NONE: No protection

View the MSTP status and statistics information.

```
<Sysname> display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge        :32768.000f-e200-2200
Bridge Times       :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC     :0.00e0-fc0e-6554 / 200200
CIST RegRoot/IRPC   :32768.000f-e200-2200 / 0
CIST RootPortId    :128.48
BPDU-Protection    :disabled
Bridge Config-
Digest-Snooping    :disabled
TC or TCN received  :2
Time since last TC  :0 days 0h:5m:42s

----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
 Port Protocol      :enabled
 Port Role          :CIST Designated Port
 Port Priority      :128
 Port Cost(Legacy)   :Config=auto / Active=200
 Desg. Bridge/Port   :32768.000f-e200-2200 / 128.2
 Port Edged         :Config=disabled / Active=disabled
 Point-to-point     :Config=auto / Active=true
 Transmit Limit     :10 packets/hello-time
 Protection Type    :None
 MST BPDU Format    :Config=auto / Active=legacy
 Port Config-
 Digest-Snooping    :disabled
 Rapid transition   :false
 Num of Vlans Mapped :1
 PortTimes          :Hello 2s MaxAge 20s FwDly 15s MsgAge 2s RemHop 20
 BPDU Sent          :186
        TCN: 0, Config: 0, RST: 0, MST: 186
 BPDU Received      :0
        TCN: 0, Config: 0, RST: 0, MST: 0

-------[MSTI 1 Global Info]-------
MSTI Bridge ID     :0.000f-e23e-9ca4
MSTI RegRoot/IRPC   :0.000f-e23e-9ca4 / 0
MSTI RootPortId    :0.0
MSTI Root Type     :PRIMARY root
Master Bridge      :32768.000f-e23e-9ca4
Cost to Master     :0
TC received        :0
```

View the MSTP status and statistics information when STP is not enabled.

```
<Sysname> display stp
 Protocol Status    :disabled
 Protocol Std.      :IEEE 802.1s
 Version           :3
```

```
CIST Bridge-Prio.  :32768
MAC address       :000f-e200-8048
Max age(s)        :20
Forward delay(s)   :15
Hello time(s)     :2
Max hops          :20
```

Table 3-3 display stp command output description

Field	Description
CIST Bridge	CIST bridge ID
Bridge Times	Major parameters for the bridge: • Hello: Hello timer • MaxAge: Max Age timer • FWDly: Forward delay timer • Max Hop: Max hops within the MST region
CIST Root/ERPC	CIST root and external path cost
CIST RegRoot/IRPC	CIST regional root and internal path cost
CIST RootPortId	CIST root port ID
BPDU-Protection	Indicates whether BPDU protection is enabled globally.
Bridge Config-Digest-Snooping	Indicates whether Digest Snooping is enabled globally on the bridge.
TC or TCN received	Number of received TC/TCN packets
Time since last TC	Time since the latest topology change
[FORWARDING]	The port learns MAC addresses and forwards user traffic
[DISCARDING]	The port does not learn MAC addresses or forward user traffic
[LEARNING]	The port learns MAC addresses but does not forward user traffic
Port Protocol	Indicates whether STP is enabled on the port
Port Role	Port role, which can be Alternate, Backup, Root, Designated, Master, or Disabled
Port Priority	Port priority
Port Cost(Legacy)	Path cost of the port. The field in the bracket indicates the standard used for port path cost calculation, which can be **legacy**, **dot1d-1998**, or **dot1t**. **Config** indicates the configured value, and **Active** indicates the actual value.
Desg. Bridge/Port	Designated bridge ID and port ID of the port The port ID displayed is insignificant for a port which does not support port priority.
Port Edged	Indicates whether the port is an edge port. **Config** indicates the configured value, and **Active** indicates the actual value.
Point-to-point	Indicates whether the port is connected to a point-to-point link. **Config** indicates the configured value, and **Active** indicates the actual value.
Transmit Limit	The maximum number of packets sent within each Hello time

Field	Description
Protection Type	Protection type on the port, which can be one of the following: • Root: Root guard • Loop: Loop guard • BPDU: BPDU guard • None: No protection
MST BPDU Format	Format of the MST BPDUs that the port can send, which can be legacy or 802.1s. **Config** indicates the configured value, and **Active** indicates the actual value.
Port Config-Digest-Snooping	Indicates whether digest snooping is enabled on the port.
Rapid transition	Indicates whether the current port rapidly transitions to the forwarding state.
Num of Vlans Mapped	Number of VLANs mapped to the current MSTI
PortTimes	Major parameters for the port: • Hello: Hello timer • MaxAge: Max Age timer • FWDly: Forward delay timer • MsgAge: Message Age timer • Remain Hop: Remaining hops
BPDU Sent	Statistics on sent BPDUs
BPDU Received	Statistics on received BPDUs
MSTI RegRoot/IRPC	MSTI regional root/internal path cost
MSTI RootPortId	MSTI root port ID
MSTI Root Type	MSTI root type, which can be primary root or secondary root
Master Bridge	MSTI root bridge ID
Cost to Master	Path cost from the MSTI to the master bridge
TC received	Number of received TC BPDUs
Protocol Status	MSTP protocol status
Protocol Std.	MSTP protocol standard
Version	MSTP protocol version
CIST Bridge-Prio.	Device priority in the CIST
MAC address	MAC address of the device
Max age(s)	Aging timer for BPDUs (in seconds)
Forward delay(s)	Port state transition delay (in seconds)
Hello time(s)	Interval for the root bridge to send BPDUs (in seconds)
Max hops	Maximum hops in the MSTI

display stp abnormal-port

Syntax

display stp abnormal-port

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display stp abnormal-port** command to view the information about abnormally blocked ports.

Any of the following reasons may cause a port to be abnormally blocked:

- Root guard function
- Loop guard function
- MSTP BPDU format incompatibility protection function

Examples

View information about abnormally blocked ports.

```
<Sysname> display stp abnormal-port
 MSTID      Blocked Port              Reason
   1        GigabitEthernet1/0/1      ROOT-Protected
   2        GigabitEthernet1/0/2      LOOP-Protected
   2        GigabitEthernet1/0/3      Formatcompatibility-Protected
```

Table 3-4 display stp abnormal-port command output description

Field	Description
MSTID	ID of the MSTI to which an abnormally blocked port belongs
Blocked Port	Name of an abnormally blocked port
Reason	Reason that caused abnormal blocking of the port. • ROOT-Protected: root guard function • LOOP-Protected: loop guard function • Formatcompatibility-Protected: MSTP BPDU format incompatibility protection function

display stp down-port

Syntax

display stp down-port

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display stp down-port** command to display the information about ports blocked by STP protection functions.

These functions include:

- BPDU attack guard function
- MSTP BPDU format frequent change protection function

Examples

View the information about ports blocked by STP protection functions.

```
<Sysname> display stp down-port
 Down Port                 Reason
 GigabitEthernet1/0/1     BPDU-Protected
 GigabitEthernet1/0/2     Formatfrequency-Protected
```

Table 3-5 display stp abnormal-port command output description

Field	Description
Down Port	Name of a blocked port
Reason	Reason that caused the port to be blocked. • BPDU-Protected: BPDU attack guard function • Formatfrequency-Protected: MSTP BPDU format frequent change protection function

display stp history

Syntax

display stp [**instance** *instance-id*] **history** [**slot** *slot-number*]

View

Any view

Default Level

0: Visit level

Parameters

instance *instance-id*: Displays the historic port role calculation information of a particular MSTI. The minimum value of *instance-id* is 0, representing the common internal spanning tree (CIST), and the maximum value of *instance-id* is 32.

slot *slot-number*: Displays the historic port role calculation information of the specified IRF member device. The slot-number argument is the member number of the device in the IRF, which you can display with the **display irf** command. The value range for the slot-number argument depends on the number of members and numbering conditions in the current IRF. If no IRF exists, the slot-number argument is the current device number.

Description

Use the **display stp history** command to view the historic port role calculation information of the specified MSTI or all MSTIs.

Note that:

- If you do not specify an MSTI ID, this command will display the historic port role calculation information of all MSTIs. The displayed information is sorted by MSTI ID, and by port role calculation time in each MSTI.
- If you specify an MSTI ID, this command will display the historic port role calculation information of only this specified MSTI by the sequence of port role calculation time.

Examples

View the historic port role calculation information of the IRF member device 1 in MSTI 2.

```
<Sysname> display stp instance 2 history slot 1
 -------------- STP slot 1 history trace ---------------
 ------------------  Instance 2   --------------------

 Port GigabitEthernet1/0/1
   Role change   : ROOT->DESI (Aged)
   Time          : 2009/02/08 00:22:56
   Port priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1

 Port GigabitEthernet1/0/2
   Role change   : ALTER->ROOT
   Time          : 2009/02/08 00:22:56
   Port priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
```

Table 3-6 display stp history command output description

Field	Description
Port	Port name
Role change	A role change of the port (“Age” means that the change was caused by expiry of the received configuration BPDU)
Time	Time of port role calculation
Port priority	Port priority

display stp region-configuration

Syntax

display stp region-configuration

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display stp region-configuration** command to view the currently effective configuration information of the MST region, including the region name, revision level, and user-configured VLAN-to-instance mappings.

Related commands: **instance**, **region-name**, **revision-level**, **vlan-mapping modulo**.

Examples

View the currently effective MST region configuration information.

```
<Sysname> display stp region-configuration
 Oper Configuration
   Format selector    :0
   Region name       :hello
   Revision level     :0

   Instance   Vlans Mapped
      0       21 to 4094
      1       1 to 10
      2       11 to 20
```

Table 3-7 display stp region-configuration command output description

Field	Description
Format selector	MSTP-defined format selector, which defaults to 0 and is not configurable
Region name	MST region name
Revision level	Revision level of the MST region, which can be configured using the **revision-level** command and defaults to 0.
Instance Vlans Mapped	VLAN-to-instance mappings in the MST region

display stp root

Syntax

display stp root

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display stp root** command to view the root bridge information of all MSTIs.

Examples

View the root bridge information of all MSTIs.

```
<Sysname> display stp root
MSTID  Root Bridge ID      ExtPathCost IntPathCost Root Port
   0   0.00e0-fc0e-6554     200200     0          GigabitEthernet1/0/1
```

Table 3-8 display stp root command output description

Field	Description
MSTID	MSTI ID
Root Bridge ID	Root bridge ID
ExtPathCost	External path cost. The device can automatically calculate the default path cost of a port, or alternatively, you can use the **stp cost** command to configure the path cost of a port.
IntPathCost	Internal path cost. The device can automatically calculate the default path cost of a port, or alternatively, you can use the **stp cost** command to configure the path cost of a port.
Root Port	Root port name (displayed only if a port of the current device is the root port of MSTIs)

display stp tc

Syntax

display stp [**instance** *instance-id*] **tc** [**slot** *slot-number*]

View

Any view

Default Level

0: Visit level

Parameters

instance *instance-id*: Displays the statistics of TC/TCN BPDUs received and sent by all ports in the specified MSTI. The minimum value of *instance-id* is 0, representing the common internal spanning tree (CIST), and the maximum value of *instance-id* is 32.

slot *slot-number*: Displays the statistics of TC/TCN BPDUs received and sent by all ports of the specified IRF member device. The slot-number argument is the member number of the device in the IRF, which you can display with the **display irf** command. The value range for the slot-number argument depends on the number of members and numbering conditions in the current IRF. If no IRF exists, the slot-number argument is the current device number.

Description

Use the **display stp tc** command to view the statistics of TC/TCN BPDUs received and sent by all ports in an MSTI or all MSTIs.

Note that:

- If you do not specify an MSTI ID, this command will display the statistics of TC/TCN BPDUs received and sent by all ports in all MSTIs. The displayed information is sorted by instance ID and by port name in each MSTI.
- If you specify an MSTI ID, this command will display the statistics of TC/TCN BPDUs received and sent by all ports in the specified MSTI, in port name order.

Examples

View the statistics of TC/TCN BPDUs received and sent by all ports on the IRF member device 1 in MSTI 0.

```
<Sysname> display stp instance 0 tc slot 1
 -------------- STP slot 1 TC or TCN count -------------
 MSTID     Port                    Receive     Send
   0       GigabitEthernet1/0/1        6         4
   0       GigabitEthernet1/0/2        0         2
```

Table 3-9 display stp tc command output description

Field	Description
MSTID	MSTI ID
Port	Port name
Receive	Number of TC/TCN BPDUs received on each port
Send	Number of TC/TCN BPDUs sent by each port

instance

Syntax

instance *instance-id* **vlan** *vlan-list*

undo instance *instance-id* [**vlan** *vlan-list*]

View

MST region view

Default Level

2: System level

Parameters

instance-id: MSTI ID. The minimum value is 0, representing the CIST, and the maximum value is 32.

vlan *vlan-list*: Specifeis a VLAN list in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id2* }*&<1-10>*, in which *vlan-id* represents the VLAN ID and ranges from 1 to 4094. *&<1-10>* indicates you can specify up to 10 VLAN IDs or VLAN ID ranges.

Description

Use the **instance** command to map the specified VLANs to the specified MSTI.

Use the **undo instance** command to remap the specified VLAN or all VLANs to the CIST (MSTI 0).

By default, all VLANs are mapped to the CIST.

Notice that:

- If you specify no VLAN in the **undo instance** command, all VLANs mapped to the specified MSTI will be remapped to the CIST.
- You cannot map the same VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping will be automatically removed.
- After configuring this command, you need to run the **active region-configuration** command to activate the VLAN-to-instance mapping.

Related commands: **display stp region-configuration**, **check region-configuration**, **active region-configuration**.

Examples

Map VLAN 2 to MSTI 1.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
```

region-name

Syntax

region-name *name*

undo region-name

View

MST region view

Default Level

2: System level

Parameters

name: MST region name, a string of 1 to 32 characters.

Description

Use the **region-name** command to configure the MST region name.

Use the **undo region-name** command to restore the default MST region name.

By default, the MST region name of a device is its MAC address.

Note that:

- The MST region name, the VLAN-to-instance mapping table and the MSTP revision level of a device jointly determine the MST region to which the device belongs.
- After configuring this command, you need to run the **active region-configuration** command to activate the configured MST region name.

Related commands: **instance**, **revision-level**, **vlan-mapping modulo**, **display stp region-configuration**, **check region-configuration**, **active region-configuration**.

Examples

Set the MST region name of the device to **hello**.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] region-name hello
```

reset stp

Syntax

reset stp [**interface** *interface-list*]

View

User view

Default Level

1: Monitor level

Parameters

interface *interface-list*: Specifies a port list, in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 ports or port ranges.

Description

Use the **reset stp** command to clear the MSTP statistics information.

The MSTP statistics information includes the numbers of TCN BPDUs, configuration BPDUs, RST BPDUs and MST BPDUs sent/received through the specified ports (STP BPDUs and TCN BPDUs are counted only for the CIST).

Note that this command clears the spanning tree-related statistics information on the specified ports if you specify the *interface-list* argument; otherwise, this command clears the spanning tree-related statistics on all ports.

Related commands: **display stp**.

Examples

Clear the spanning tree-related statistics information on ports GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3.

```
<Sysname> reset stp interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

revision-level

Syntax

revision-level *level*

undo revision-level

View

MST region view

Default Level

2: System level

Parameters

level: MSTP revision level, in the range of 0 to 65535.

Description

Use the **region-level** command to configure the MSTP revision level.

Use the **undo region-level** command to restore the default MSTP revision level.

By default, the MSTP revision level is 0.

Note that:

- The MSTP revision level, the MST region name and the VLAN-to-instance mapping table of a device jointly determine the MST region to which the device belongs. When the MST region name and VLAN-to-instance mapping table are both the same for two MST regions, you can still tell them apart by their MSTP revision levels.
- After configuring this command, you need to run the **active region-configuration** command to activate the configured MST region level.

Related commands: **instance**, **region-name**, **vlan-mapping modulo**, **display stp region-configuration**, **check region-configuration**, **active region-configuration**.

Examples

Set the MSTP revision level of the MST region to 5.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] revision-level 5
```

stp bpdu-protection

Syntax

stp bpdu-protection

undo stp bpdu-protection

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **stp bpdu-protection** command to enable the BPDU guard function.

Use the **undo stp bpdu-protection** command to disable the BPDU guard function.

By default, the BPDU guard function is disabled.

Examples

Enable the BPDU guard function.

```
<Sysname> system-view
[Sysname] stp bpdu-protection
```

stp bridge-diameter

Syntax

stp bridge-diameter *diameter*

undo stp bridge-diameter

View

System view

Default Level

2: System level

Parameters

diameter: Specifies the switched network diameter, in the range of 2 to 7.

Description

Use the **stp bridge-diameter** command to specify the network diameter, namely the maximum possible number of stations between any two terminal devices on the switched network.

Use the **undo stp bridge-diameter** command to restore the default.

By default, the network diameter of the switched network is 7.

Note that:

- An appropriate setting of hello time, forward delay and max age can speed up network convergence. The values of these timers are related to the network size. You can set these three timers indirectly by setting the network diameter. Based on the network diameter you configured, MSTP automatically sets an optimal hello time, forward delay, and max age for the device. With the network diameter set to 7 (the default), the three timer are also set to their defaults.
- This configuration must be configured on the root bridge and is effective for the CIST only, not for MSTIs.

Related commands: **stp timer forward-delay**, **stp timer hello**, **stp timer max-age**.

Examples

Set the network diameter of the switched network to 5.

```
<Sysname> system-view
[Sysname] stp bridge-diameter 5
```

stp compliance

Syntax

stp compliance { **auto** | **dot1s** | **legacy** }

undo stp compliance

View

Ethernet interface view, port group view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

auto: Configures the port(s) to recognize the MSTP BPDU format automatically and accordingly determine the format of MSTP BPDUs to send.

dot1s: Configures the port(s) to receive and send only standard-format (802.1s-compliant) MSTP BPDUs.

legacy: Configures the port(s) to receive and send only compatible-format MSTP BPDUs.

Description

Use the **stp compliance** command to configure the mode the specified port(s) will use to recognize and send MSTP BPDUs.

Use the **undo stp compliance** command to restore the system default.

By default, a port automatically recognizes the formats of received MSTP packets and determines the formats of MSTP packets to be sent based on the recognized formats.

Note that:

- Configured in Ethernet interface view, the setting takes effect on the current interface only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface; configured on a member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group.

Examples

Configure GigabitEthernet 1/0/1 to receive and send only standard-format (802.1s) MSTP packets.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp compliance dot1s
```

stp config-digest-snooping

Syntax

stp config-digest-snooping

undo stp config-digest-snooping

View

System view, Ethernet interface view, port group view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

None

Description

Use the **stp config-digest-snooping** command to enable Digest Snooping.

Use the **undo stp config-digest-snooping** command to disable Digest Snooping.

The feature is disabled by default.

Note that:

- Configured in system view, the setting takes effect globally; configured in Ethernet interface view, the setting takes effect on the current interface only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface; configured on a member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group.
- You need to enable this feature both globally and on ports connected to third-party devices to make it take effect. It is recommended to enable the feature on all associated ports first and then globally, making all configured ports take effect at the same time to minimize the impact on the network, and disable the feature globally to disable it on all associated ports.

Related commands: **display stp**.

Examples

Enable Digest Snooping on GigabitEthernet 1/0/1 and then globally.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp config-digest-snooping
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] stp config-digest-snooping
```

stp cost

Syntax

stp [**instance** *instance-id*] **cost** *cost*

undo stp [**instance** *instance-id*] **cost**

View

Ethernet interface view, port group view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

instance *instance-id*: Sets the path cost of the port(s) in a particular MSTI. The minimum value of *instance-id* is 0, representing the CIST, and the maximum value of *instance-id* is 32.

cost: Path cost of the port, the effective range of which depends on the path cost calculation standard adopted.

- With the IEEE 802.1d-1998 standard selected for path cost calculation, the *cost* argument ranges from 1 to 65535.
- With the IEEE 802.1t standard selected for path cost calculation, the *cost* argument ranges from 1 to 200000000.
- With the private standard selected for path cost calculation, the *cost* argument ranges from 1 to 200000.

Description

Use the **stp cost** command to set the path cost of the port(s) in the specified MSTI or all MSTIs.

Use the **undo stp cost** command to restore the system default.

By default, the device automatically calculates the path costs of ports in each MSTI based on the corresponding standard.

Note that:

- Configured in Ethernet interface view, the setting takes effect on the current interface only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface; configured on a member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group.
- Path cost is an important factor in spanning tree calculation. Setting different path costs for a port in MSTIs allows VLAN traffic flows to be forwarded along different physical links, thus achieving VLAN-based load balancing.
- The path cost setting of a port can affect the role selection of the port. When the path cost of a port is changed, MSTP will re-compute the role of the port and initiate a state transition.

Related commands: **display stp**.

Examples

Set the path cost of port GigabitEthernet 1/0/3 in MSTI 2 to 200.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] stp instance 2 cost 200
```

stp edged-port

Syntax

stp edged-port { **enable** | **disable** }

undo stp edged-port

View

Ethernet interface view, port group view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

enable: Configures the current port(s) to be an edge port or edge ports.

disable: Configures the current port(s) to be a non-edge port or non-edge ports.

Description

Use the **stp edged-port enable** command to configure the port(s) as an edge port or ports.

Use the **undo stp edged-port** command to restore the default.

All ports are non-edge ports by default.

Note that:

- Configured in Ethernet interface view, the setting takes effect on the current interface only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface; configured on a member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group.
- If a port directly connects to a user terminal rather than another device or a shared LAN segment, this port is regarded as an edge port. When the network topology changes, an edge port will not cause a temporary loop. Therefore, configuring a port as an edge port can enable the port to transition to the forwarding state rapidly. We recommend that you configure a port directly connecting to a user terminal as an edge port to enable it to transition to the forwarding state rapidly.
- Normally, configuration BPDUs from other devices cannot reach an edge port because it does not connect to any other device. Before the BPDU guard function is enabled, if a port receives a configuration BPDU, the port is working actually as a non-edge port even if you have configured it as an edge port.

Examples

Configure GigabitEthernet 1/0/1 as an edge port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp edged-port enable
```

stp enable

Syntax

stp enable

undo stp enable

View

System view, Ethernet interface view, port group view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

None

Description

Use the **stp enable** command to enable MSTP globally in system view, on a port in interface view, or on multiple ports in port group view.

Use the **undo stp enable** command to disable MSTP globally or on the port(s).

By default, MSTP is enabled on all ports and globally.

Note that:

- MSTP takes effect when it is enabled both globally and on the port.
- Configured in system view, the setting takes effect globally; configured in Ethernet interface view, the setting takes effect on the current interface only; configured in port group view, the setting takes effect on all ports in the port group; configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface; configured on a member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group.
- After you enable MSTP, the device works in STP-compatible mode, RSTP mode or MSTP mode depending on the MSTP mode setting.
- After being enabled, MSTP dynamically maintains the spanning tree status of VLANs based on received configuration BPDUs; after being disabled, it stops maintaining the spanning tree status.

Related commands: **stp mode**.

Examples

Disable the MSTP feature globally.

```
<Sysname> system-view
[Sysname] undo stp enable
```

Disable MSTP on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
```

stp loop-protection

Syntax

stp loop-protection

undo stp loop-protection

View

Ethernet interface view, port group view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

None

Description

Use the **stp loop-protection** command to enable the loop guard function on the port(s).

Use the **undo stp loop-protection** command to restore the system default.

By default, the loop guard function is disabled.

Note that:

- Configured in Ethernet interface view, the setting takes effect on the current interface only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group.

Examples

Enable the loop guard function on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp loop-protection
```

stp max-hops

Syntax

stp max-hops *hops*

undo stp max-hops

View

System view

Default Level

2: System level

Parameters

hops: Maximum hops, in the range of 1 to 40

Description

Use the **stp max-hops** command to set the maximum hops of the MST region on the device.

Use the **undo stp max-hops** command to restore the maximum hops to the default setting.

Setting the maximum hops of MST regions is to limit the sizes of MST regions. By default, the maximum number of hops of an MST region is 20.

Related commands: **display stp**.

Examples

Set the maximum hops of the MST region on the device to 35.

```
<Sysname> system-view
[Sysname] stp max-hops 35
```

stp mcheck

Syntax

stp mcheck

View

System view, Ethernet interface view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

None

Description

Use the **stp mcheck** command to carry out the mCheck operation globally or on the current port.

If a port on a device running MSTP (or RSTP) connects to a device running STP, this port will automatically migrate to the STP-compatible mode. However, it will not be able to migrate automatically back to the MSTP (or RSTP) mode, but will remain working in the STP-compatible mode under the following circumstances:

- The device running STP is shut down or removed.
- The device running STP migrates to the MSTP (or RSTP) mode.

By then, you can perform an mCheck operation to force the port to migrate to the MSTP (or RSTP) mode.

Note that:

- The device works in STP-compatible mode, RSTP mode or MSTP mode depending on the MSTP mode setting.
- The **stp mcheck** command is meaningful only when the device works in RSTP or MSTP mode.
- Configured in system view, the setting takes effect globally; configured in Ethernet interface view, the setting takes effect on the current interface only; configured in port group view, the setting takes effect on all member ports in the port group.
- Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface; configured on a member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group.

Related commands: **stp mode**.

Examples

Carry out mCheck on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp mcheck
```

stp mode

Syntax

stp mode { **stp** | **rstp** | **mstp** }

undo stp mode

View

System view

Default Level

2: System level

Parameters

stp: Configures the MSTP-enabled device to work in STP-compatible mode.

rstp: Configures an MSTP-enabled device to work in RSTP mode.

mstp: Configures an MSTP-enabled device to work in MSTP mode.

Description

Use the **stp mode** command to configure the MSTP work mode of the device.

Use the **undo stp mode** command to restore the MSTP work mode to the default setting.

By default, an MSTP-enabled device works in MSTP mode.

Related commands: **stp mcheck**, **stp enable**.

Examples

Configure the MSTP-enabled device to work in STP-compatible mode.

```
<Sysname> system-view
[Sysname] stp mode stp
```

stp no-agreement-check

Syntax

stp no-agreement-check

undo stp no-agreement-check

View

Ethernet interface view, port group view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

None

Description

Use the **stp no-agreement-check** command to enable No Agreement Check on the port(s).

Use the **undo stp no-agreement-check** command to disable No Agreement Check on the port(s).

By default, No Agreement Check is disabled.

Note that:

- Configured in Ethernet interface view, the setting takes effect on the current interface only; configured in port group view, the setting takes effect on all member ports in the port group.
- Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface; configured on a member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group.
- This feature takes effect only after you enable it on the root port.

Examples

Enable No Agreement Check on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp no-agreement-check
```

stp pathcost-standard

Syntax

stp pathcost-standard { **dot1d-1998** | **dot1t** | **legacy** }

undo stp pathcost-standard

View

System view

Default Level

2: System level

Parameters

dot1d-1998: The device calculates the default path cost for ports based on IEEE 802.1d-1998.

dot1t: The device calculates the default path cost for ports based on IEEE 802.1t.

legacy: The device calculates the default path cost for ports based on a private standard.

Description

Use the **stp pathcost-standard** command to specify a standard for the device to use when calculating the default path costs for ports of the device.

Use the **undo stp pathcost-standard** command to restore the system default.

By default, the device calculates the default path cost for ports based on a private standard.

Note that:

- If you change the standard that the device uses in calculating the default path cost, the port path cost value set through the **stp cost** command will be invalid.
- Table 3-10 shows the path costs calculated using different standards at different link speed. When calculating path cost for an aggregate interface, 802.1d-1998 does not take into account the number of member ports in its aggregation group as 802.1t does. The calculation formula of 802.1t is: Path Cost = 200,000,000/link speed (in 100 kbps), where link speed is the sum of the link speed values of the non-blocked ports in the aggregation group.

Table 3-10 Link speed vs. path cost

Link speed	Duplex state	Path cost in 802.1d-1998 standard	Path cost in IEEE 802.1t standard	Path cost in private standard
0	—	65535	200,000,000	200,000
10 Mbps	Single Port Aggregate Link 2 Ports Aggregate Link 3 Ports Aggregate Link 4 Ports	100 100 100 100	2,000,000 1,000,000 666,666 500,000	2,000 1,800 1,600 1,400
100 Mbps	Single Port Aggregate Link 2 Ports Aggregate Link 3 Ports Aggregate Link 4 Ports	19 19 19 19	200,000 100,000 66,666 50,000	200 180 160 140
1000 Mbps	Single Port Aggregate Link 2 Ports Aggregate Link 3 Ports Aggregate Link 4 Ports	4 4 4 4	20,000 10,000 6,666 5,000	20 18 16 14
10 Gbps	Single Port Aggregate Link 2 Ports Aggregate Link 3 Ports Aggregate Link 4 Ports	2 2 2 2	2,000 1,000 666 500	2 1 1 1

Related commands: **stp cost**, **display stp**.

Examples

Configure the device to calculate the default path cost for ports based on IEEE 802.1d-1998.

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1d-1998
```

stp point-to-point

Syntax

stp point-to-point { **auto** | **force-false** | **force-true** }

undo stp point-to-point

View

Ethernet interface view, port group view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

auto: Specifies automatic detection of the link type.

force-false: Specifies the non-point-to-point link type.

force-true: Specifies the point-to-point link type.

Description

Use the **stp point-to-point** command to configure the link type of the current port(s).

Use the **undo stp point-to-point** command to restore the system default.

The default setting is **auto**; namely the MSTP-enabled device automatically detects whether a port connects to a point-to-point link.

Note that:

- Configured in Ethernet interface view, the setting takes effect on the current interface only; configured in port group view, the setting takes effect on all member ports in the port group.
- Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on a member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group.
- When connecting to a non-point-to-point link, a port is incapable of rapid state transition.
- If the current port is a Layer 2 aggregate interface or if it works in full duplex mode, the link to which the current port connects is a point-to-point link. We recommend that you use the default setting, namely let MSTP detect the link status automatically.
- This setting takes effect on the CIST and all MSTIs. If a port is configured as connecting to a point-to-point link or a non-point-to-point link, the setting takes effect for the port in all MSTIs. If the physical link to which the port connects is not a point-to-point link and you force it to be a point-to-point link by configuration, your configuration may incur a temporary loop.

Related commands: **display stp**.

Examples

Configure the link connecting GigabitEthernet 1/0/3 as a point-to-point link.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] stp point-to-point force-true
```

stp port priority

Syntax

stp [**instance** *instance-id*] **port priority** *priority*

undo stp [**instance** *instance-id*] **port priority**

View

Ethernet interface view, port group view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

instance *instance-id*: Sets the priority of the current port(s) in a particular MSTI. The minimum value of *instance-id* is 0, representing the CIST, and the maximum value of *instance-id* is 32.

priority: Port priority, in the range of 0 to 240 at the step of 16 (0, 16, 32…, for example).

Description

Use the **stp port priority** command to set the priority of the port(s).

Use the **undo stp port priority** command to restore the system default.

Port priority affects the role of a port in an MSTI.

By default, the port priority is 128.

Note that:

- Configured in Ethernet interface view, the setting takes effect on the current interface only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on a member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group.
- Setting different priorities for the same port in different MSTIs allows VLAN traffic flows to be forwarded along different physical links, thus to achieve VLAN-based load balancing.
- When the priority of a port is changed in an MSTI, MSTP will re-compute the role of the port and initiate a state transition in the MSTI.

Related commands: **display stp**.

Examples

Set the priority of port GigabitEthernet 1/0/3 in MSTI 2 to 16.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/3
[Sysname-GigabitEthernet1/0/3] stp instance 2 port priority 16
```

stp port-log

Syntax

stp port-log { **all | instance** *instance-id* }

undo stp port-log { **all | instance** *instance-id* }

View

System view

Default Level

2: System level

Parameters

all: Enables output of port state transition information for all MSTIs.

instance *instance-id*: Enables output of port state transition information for the specified MSTI. The minimum value of *instance-id* is 0, representing the CIST, and the maximum value of this argument is 32.

Description

Use the **stp port-log** command to enable output of port state transition information for the specified MSTI or all MSTIs.

Use the **undo stp port-log** command to disable output of port state transition information for the specified MSTI or all MSTIs.

This function is enabled by default.

Examples

Enable output of port state transition information for MSTI 2.

```
<Sysname> system-view
[Sysname] stp port-log instance 2
%Aug 16 00:49:41:856 2006 Sysname MSTP/3/PDISC: Instance 2's GigabitEthernet1/0/1 has been set to discarding state!
%Aug 16 00:49:41:856 2006 Sysname MSTP/3/PFWD: Instance 2's GigabitEthernet1/0/2 has been set to forwarding state!
```

// The information above shows that in MSTI 2 the state of GigabitEthernet 1/0/1 has changed to discarding and that of GigabitEthernet 1/0/2 has changed to forwarding.

stp priority

Syntax

stp [**instance** *instance-id*] **priority** *priority*

undo stp [**instance** *instance-id*] **priority**

View

System view

Default Level

2: System level

Parameters

instance *instance-id*: Sets the priority of the device in a MSTI. The minimum value of *instance-id* is 0, representing the CIST, and the maximum value of *instance-id* is 32.

priority: Device priority, in the range of 0 to 61440 at the step of 4096, namely you can set up to 16 priority values, such as 0, 4096, 8192…, on the device. The smaller the *priority* value, the higher the device priority.

Description

Use the **stp priority** command to set the priority of the device.

Use the **undo stp priority** command to restore the default device priority.

By default, the device priority is 32768.

Examples

Set the device priority in MSTI 1 to 4096.

```
<Sysname> system-view
[Sysname] stp instance 1 priority 4096
```

stp region-configuration

Syntax

stp region-configuration

undo stp region-configuration

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **stp region-configuration** command to enter MST region view.

Use the **undo stp region-configuration** command to restore the default MST region configurations.

By default, the default settings are used for all the three MST region parameters. Namely, the device's MST region name is the device's MAC address, all VLANs are mapped to the CIST, and the MSTP revision level is 0.

After you enter MST region view, you can configure the MST region-related parameters, including the region name, VLAN-to-instance mappings and revision level.

Examples

Enter MST region view.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region]
```

stp root primary

Syntax

stp [**instance** *instance-id*] **root primary**

undo stp [**instance** *instance-id*] **root**

View

System view

Default Level

2: System level

Parameters

instance *instance-id*: Configures the device as the root bridge in a particular MSTI. The minimum value of *instance-id* is 0, representing the CIST, and the maximum value of *instance-id* is 32.

Description

Use the **stp root primary** command to configure the current device as the root bridge.

Use the **undo stp root** command to restore the system default.

By default, a device is not a root bridge in any MSTI.

Note that:

- There is only one root bridge in effect in an MSTI. If two or more devices have been designated to be root bridges of the same MSTI, MSTP will select the device with the lowest MAC address as the root bridge.
- You can specify a root bridge for each MSTI without caring about the device priority. After specifying the current device as the root bridge or a secondary root bridge, you cannot change the priority of the device.

Related commands: **stp priority**, **stp root secondary**.

Examples

Specify the current device as the root bridge of MSTI 0.

```
<Sysname> system-view
[Sysname] stp instance 0 root primary
```

stp root secondary

Syntax

stp [**instance** *instance-id*] **root secondary**

undo stp [**instance** *instance-id*] **root**

View

System view

Default Level

2: System level

Parameters

instance *instance-id*: Configures the device as a secondary root bridge in a particular MSTI. The minimum value of *instance-id* is 0, representing the CIST, and the maximum value of *instance-id* is 32.

Description

Use the **stp root secondary** command to configure the device as a secondary root bridge.

Use the **undo stp root** command to restore the system default.

By default, a device is not a secondary root bridge.

Note that:

- You can configure one or more secondary root bridges for each MSTI. When the root bridge of an MSTI fails or is shut down, the secondary root bridge can take over the role of the root bridge of the specified MSTI. However, if you specify a new primary root bridge for the instance then, the secondary root bridge will not become the root bridge. If you specify more than one secondary root bridge, the secondary root bridge with the lowest MAC address will become the root bridge.

- After specifying the current device as a secondary root bridge, you cannot change the priority of the device.

Related commands: **stp priority**, **stp root primary**.

Examples

Specify the current device as a secondary root bridge of MSTI 0.

```
<Sysname> system-view
[Sysname] stp instance 0 root secondary
```

stp root-protection

Syntax

stp root-protection

undo stp root-protection

View

Ethernet interface view, port group view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

None

Description

Use the **stp root-protection** command to enable the root guard function on the port(s).

Use the **undo stp root-protection** command to restore the default.

By default, the root guard function is disabled.

Note that:

- Configured in Ethernet interface view, the setting takes effect on the current interface only; configured in port group view, the setting takes effect on all ports in the port group.
- Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface. Configured on the member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group.

Examples

Enable the root guard function for GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp root-protection
```

stp tc-protection

Syntax

stp tc-protection enable

stp tc-protection disable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **stp tc-protection enable** command to enable the TC-BPDU attack guard function for the device.

Use the **stp tc-protection disable** command to disable the TC-BPDU attack guard function for the device.

By default, the TC-BPDU attack guard function is enabled.

Examples

Disable the TC-BPDU attack guard function for the device.

```
<Sysname> system-view
[Sysname] stp tc-protection disable
```

stp tc-protection threshold

Syntax

stp tc-protection threshold *number*

undo stp tc-protection threshold

View

System view

Default Level

2: System level

Parameters

number: Maximum number of immediate forwarding address entry flushes that the switch can perform within a certain period of time after it receives the first TC-BPDU. The value range for the argument is 1 to 255.

Description

Use the **stp tc-protection threshold** command to configure the maximum number of forwarding address entry flushes that the device can perform within a certain period of time after it receives the first TC-BPDU.

Use the **undo stp tc-protection threshold** command to restore the default.

By default, the device can perform a maximum of six forwarding address entry flushes within 10 seconds after it receives the first TC-BPDU.

Examples

Set the maximum number of forwarding address entry flushes that the device can perform within 10 seconds after it receives the first TC-BPDU to 10.

```
<Sysname> system-view
[Sysname] stp tc-protection threshold 10
```

stp timer forward-delay

Syntax

stp timer forward-delay *time*

undo stp timer forward-delay

View

System view

Default Level

2: System level

Parameters

time: Forward delay in centiseconds, ranging form 400 to 3000 at the step of 100.

Description

Use the **stp timer forward-delay** command to set the forward delay timer of the device.

Use the **undo stp timer forward-delay** command to restore the system default.

By default, the forward delay timer is set to 1,500 centiseconds.

In order to prevent temporary loops, a port must go through an intermediate state, the learning state, before it transitions from the discarding state to the forwarding state, and must wait a certain period of time before it transitions from one state to another to keep synchronized with the remote device during state transition. The forward delay timer set on the root bridge determines the time interval of state transition.

If the current device is the root bridge, the state transition interval of the device depends on the forward delay value configured through this command; for a non- root bridge, its state transition interval is determined by the forward delay timer set on the root bridge.

The settings of the hello time, forward delay and max age timers must meet the following formulae, thus avoiding frequent network changes:

- 2 × (forward delay – 1 second) ⩾ max age
- Max age ⩾ 2 × (hello Time + 1 second)

We recommend that you specify the network diameter of the switched network using the **stp root primary** command and let MSTP automatically calculate optimal settings of these three timers.

Related commands: **stp timer hello**, **stp timer max-age**, **stp bridge-diameter**.

Examples

Set the forward delay timer of the device to 2,000 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer forward-delay 2000
```

stp timer hello

Syntax

stp timer hello *time*

undo stp timer hello

View

System view

Default Level

2: System level

Parameters

time: Hello time in centiseconds, ranging from 100 to 1000 at the step of 100.

Description

Use the **stp timer hello** command to set the hello time of the device.

Use the **undo stp timer hello** command to restore the system default.

By default, the hello time is set to 200 centiseconds.

Hello time is the time interval at which MSTP-enabled devices send configuration BPDUs to maintain spanning tree. If a device fails to receive configuration BPDUs within the set period of time, a new spanning tree calculation process will be triggered due to timeout. The root bridge sends configuration BPDUs at the interval of the hello time set through this command, while non-root bridges use the hello time set on the root bridge.

The settings of the hello time, forward delay and max age timers must meet the following formulae, thus avoiding frequent network changes:

- 2 × (forward delay – 1 second) ⩾ max age
- Max age ⩾ 2 × (hello time + 1 second)

We recommend that you specify the network diameter of the switched network using the **stp root primary** command and let MSTP automatically calculate optimal settings of these three timers.

Related commands: **stp timer forward-delay**, **stp timer max-age**, **stp bridge-diameter**.

Examples

Set the hello time of the device to 400 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer hello 400
```

stp timer max-age

Syntax

stp timer max-age *time*

undo stp timer max-age

View

System view

Default Level

2: System level

Parameters

time: Max age in centiseconds, ranging from 600 to 4000 at the step of 100.

Description

Use the **stp timer max-age** command to set the max age timer of the device.

Use the **undo stp timer max-age** command to restore the system default.

By default, the max age is set to 2,000 centiseconds.

MSTP can detect link failures and automatically restore the forwarding state of the redundant link. In the CIST, the device determines whether a configuration BPDU received on a port has expired based on the max age timer. If a port receives a configuration BPDU that has expired, that MSTI needs to be re-computed.

The max age timer is not meaningful for MSTIs. If the current device is the root bridge of the CIST, it determines whether a configuration BPDU has expired based on the configured max age timer; if the current device is not the root bridge of the CIST, it uses the max age timer set on the CIST root bridge.

The settings of the hello time, forward delay and max age timers must meet the following formulae, thus avoiding frequent network changes:

- 2 × (forward delay – 1 second) ⩾ max age
- Max age ⩾ 2 × (hello time + 1 second)

We recommend that you specify the network diameter using the **stp root primary** command and let MSTP automatically calculate an optimal setting of these three timers.

Related commands: **stp timer forward-delay**, **stp timer hello**, **stp bridge-diameter**.

Examples

Set the max age timer of the device to 1,000 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer max-age 1000
```

stp timer-factor

Syntax

stp timer-factor *factor*

undo stp timer-factor

View

System view

Default Level

2: System level

Parameters

factor: Timeout factor, in the range of 1 to 20.

Description

Use the **stp timer-factor** command to set the timeout factor, which decides the timeout time. Timeout time = timeout factor × 3 × hello time.

Use the **undo stp timer-factor** command to restore the default.

By default, the timeout factor is 3.

Note that:

- After the network topology is stabilized, each non-root-bridge device forwards configuration BPDUs to the surrounding devices at the interval of hello time to check whether any link is faulty. Typically, if a device does not receive a BPDU from the upstream device within nine times the hello time, it will assume that the upstream device has failed and start a new spanning tree calculation process.
- In a very stable network, this kind of spanning tree calculation may occur because the upstream device is busy. In this case, you can avoid such unwanted spanning tree calculations by lengthening the timeout time, thus saving the network resources. We recommend that you set the timeout factor to 5, or 6, or 7 for a stable network.

Examples

Set the timeout factor of the device to 7.

```
<Sysname> system-view
[Sysname] stp timer-factor 7
```

stp transmit-limit

Syntax

stp transmit-limit *limit*

undo stp transmit-limit

View

Ethernet interface view, port group view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

limit: Maximum number of BPDUs the port(s) can send within each hello time, in the range of 1 to 255.

Description

Use the **stp transmit-limit** command to set the maximum transmission rate of the port(s), that is, the maximum number of BPDUs the port(s) can send within each hello time.

Use the **undo stp transmit-limit** command to restore the system default.

By default, the maximum transmission rate of all ports of the device is 10, that is, each port can send up to 10 BPDUs within each hello time.

Note that:

- Configured in Ethernet interface view, the setting takes effect on the current interface only; configured in port group view, the setting takes effect on all member ports in the port group.
- Configured in Layer 2 aggregate interface view, the setting takes effect only on the aggregate interface; configured on a member port in an aggregation group, the setting can take effect only after the port leaves the aggregation group.
- A larger maximum transmission rate value represents more BPDUs that the port will send within each hello time, but this means that more system resources will be used. An appropriate maximum transmission rate setting can limit the speed at which a port sends BPDUs and prevent MSTP from using excessive bandwidth resources during network topology changes. You are recommended to use the default value.

Examples

Set the maximum transmission rate of port GigabitEthernet 1/0/1 to 5.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp transmit-limit 5
```

vlan-mapping modulo

Syntax

vlan-mapping modulo *modulo*

View

MST region view

Default Level

2: System level

Parameters

modulo: Modulo value. The minimum value is 1, and the maximum value is 32.

Description

Use the **vlan-mapping modulo** command to map VLANs in the current MST region to MSTIs according to the specified modulo value, thus quickly creating a VLAN-to-instance mapping table.

By default, all VLANs are mapped to the CIST (MSTI 0).

Note that:

- You cannot map the same VLAN to different MSTIs. If you map a VLAN that has been mapped to an MSTI to a new MSTI, the old mapping will be automatically removed.

- This command maps each VLAN to the MSTI whose ID is (VLAN ID–1) %*modulo* + 1, where (VLAN ID-1) %*modulo* is the modulo operation for (VLAN ID–1). If the modulo value is 15, for example, then VLAN 1 will be mapped to MSTI 1, VLAN 2 to MSTI 2, VLAN 15 to MSTI 15, VLAN 16 to MSTI 1, and so on.

Related commands: **region-name**, **revision-level**, **display stp region-configuration**, **check region-configuration**, **active region-configuration**.

Examples

Map VLANs to MSTIs as per modulo 8.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] vlan-mapping modulo 8
```

4 LLDP Configuration Commands

LLDP Configuration Commands

display lldp local-information

Syntax

display lldp local-information [**global** | **interface** *interface-type interface-number*]

View

Any view

Default level

1: Monitor level

Parameters

global: Displays the global LLDP information to be transmitted.

interface *interface-type interface-number*: Displays the LLDP information to be sent out the interface specified by its type and number.

Description

Use the **display lldp local-information** command to display the global LLDP information to be transmitted, which will be contained in the LLDP TLVs and sent to neighbor devices.

If no keyword or argument is specified, this command displays all the LLDP information to be sent, including the global LLDP information and the LLDP information about the LLDP-enabled ports in the up state.

Examples

Display all the LLDP information to be sent.

```
<Sysname> display lldp local-information
Global LLDP local-information:
  Chassis ID        : 00e0-fc00-5600
  System name       : System
  System description : System
  System capabilities supported : Bridge,Router
  System capabilities enabled   : Bridge,Router

  MED information
  Device class: Connectivity device

  (MED inventory information of master board)
  HardwareRev             : REV.A
```

```
  FirmwareRev            : 109
  SoftwareRev            : 5.20 Alpha 2101
  SerialNum              : NONE
  Manufacturer name       : Manufacturer name
  Model name             : Model name
  Asset tracking identifier : Unknown
LLDP local-information of port 1[GigabitEthernet1/0/1]:
  Port ID subtype  : Interface name
  Port ID        : GigabitEthernet1/0/1
  Port description : GigabitEthernet1/0/1 Interface

  Management address type         : ipv4
  Management address             : 192.168.1.11
  Management address interface type : IfIndex
  Management address interface ID   : 54
  Management address OID          : 0

  Port VLAN ID(PVID): 1

  Port and protocol VLAN ID(PPVID) : 1
  Port and protocol VLAN supported : Yes
  Port and protocol VLAN enabled   : No

  VLAN name of VLAN 1: VLAN 0001
  Auto-negotiation supported : Yes
  Auto-negotiation enabled   : Yes
  OperMau                : speed(1000)/duplex(Full)

  Power port class        : PSE
  PSE power supported      : Yes
  PSE power enabled       : No
  PSE pairs control ability : No
  Power pairs            : Signal
  Port power classification : Class 0

  Link aggregation supported : Yes
  Link aggregation enabled   : No
  Aggregation port ID       : 0

  Maximum frame Size: 1536

  MED information
  Media policy type       : Unknown
  Unknown Policy         : Yes
  VLAN tagged            : No
  Media policy VlanID     : 0
  Media policy L2 priority : 0
```

```
Media policy Dscp       : 0

PoE PSE power source     : Primary
Port PSE Priority        : Low
Port Available power value: 15.4(w)
```

Table 4-1 display lldp local-information command output description

Field	Description
Global LLDP local-information	The global LLDP information to be sent
Chassis ID	ID that identifies the LLDP sending device, which can be a MAC address, a network address, an interface or some other value depending on the chassis type.
System name	System name
System description	System description
System capabilities supported	Supported capabilities, which can be: • Bridge, indicating switching • Router, indicating routing
System capabilities enabled	Currently enabled capabilities, which can be: • Bridge, indicating switching is currently enabled. • Router, indicating routing is currently enabled.
MED information	MED information
Device class	Device type, which can be: • Connectivity device, indicating an intermediate device. • Class I, indicating a normal terminal device. All terminal devices that are LLDP-enabled are of this type. • Class II, indicating a media terminal device. A device of this type is media-capable. That is, besides the capabilities of a normal terminal device, it also supports media streams. • Class III indicating a communication terminal device. A device of this type supports IP communication systems of end user. A device of this type supports all the capabilities of a normal terminal device and a media terminal device and can be used directly by end users.
MED inventory information of master board	MED inventory information of the master device in an IRF
HardwareRev	Hardware version
FirmwareRev	Firmware version
SoftwareRev	Software version
SerialNum	Serial number
Manufacturer name	Device manufacturer
Model name	Device model
Asset tracking identifier	Asset tracking ID
LLDP local-information of port 1	LLDP information to be sent out port 1
Port ID subtype	Port ID type, which can be MAC address or interface name
Port ID	Port ID, the value of which depends on the port ID type

Field	Description
Port description	Port description
Management address type	Management address type
Management address	Management address
Management address interface type	Type of the interface identified by the management address
Management address interface ID	ID of the interface identified by the management address
Management address OID	Management address object ID
Port VLAN ID(PVID)	Port VLAN ID
Port and protocol VLAN ID(PPVID)	Port protocol VLAN ID
Port and protocol VLAN supported	Indicates whether protocol VLAN is supported on the port.
Port and protocol VLAN enabled	Indicates whether protocol VLAN is enabled on the port.
VLAN name of VLAN 1	Name of VLAN 1
Auto-negotiation supported	Indicates whether auto-negotiation is supported on the port.
Auto-negotiation enabled	State of auto-negotiation
OperMau	Current speed and duplex state of the port
PoE supported	Indicates whether PoE is supported on the port.
Power port class	PoE device type, which can be : • PSE: power sourcing equipment • PD: powered device
PSE power supported	Indicates whether or not the device can operate as a PSE.
PSE power enabled	Indicates whether or not the device is operating as a PSE.
PSE pairs control ability	Indicates whether or not the PSE-PD pair control is available.
Power pairs	PoE mode, which can be **Signal** (PoE via signal lines) or **Spare** (PoE via spare lines).
Port power classification	Port power classification of the PD, which can be: • Class0 • Class1 • Class2 • Class3 • Class4
Link aggregation supported	Indicates whether or not link aggregation is supported.
Link aggregation enabled	Indicates whether or not link aggregation is enabled.
Aggregation port ID	Aggregation group ID, which is 0 if link aggregation is not enabled.
Maximum frame Size	Maximum frame size supported
MED information	MED LLDP information

Field	Description
Media policy type	Media policy type, which can be: • unknown • voice • voiceSignaling • guestVoice • guestVoiceSignaling • softPhoneVoice • videoconferencing • streamingVideo • videoSignaling
Unknown Policy	Indicates whether or not the media policy is unknown.
VLAN tagged	Indicates whether packets of the media VLAN are tagged.
Media Policy VlanID	ID of the media VLAN
Media Policy L2 priority	Layer 2 priority
Media Policy Dscp	DSCP precedence
Location format	Location information format, which can be: • Invalid, indicating the format of the location information is invalid. • Coordinate-based LCI, indicating the location information is coordinate-based. • Civic Address LCI, indicating normal address information. • ECS ELIN, indicating a telephone number for urgencies.
Location Information	Location information
PoE PSE power source	PSE power type, which can be: • Primary, indicating a primary power supply • Backup, indicating a backup power supply
Port PSE Priority	PoE power supply priority of PSE ports, which can be: • Unknown • Critical • High • Low
Port available power value	Available PoE power on PSE ports

display lldp neighbor-information

Syntax

display lldp neighbor-information [**brief** | **interface** *interface-type interface-number* [**brief**] | **list** [**system-name** *system-name*]]

View

Any view

Default level

1: Monitor level

Parameters

brief: Displays the brief LLDP information sent by the neighboring devices. If the **brief** keyword is not specified, this command displays the detailed LLDP information sent by the neighboring devices.

interface *interface-type interface-number*: Displays the LLDP information about the neighboring devices received through a port specified by its type and number. If this keyword-argument combination is not specified, this command displays the LLDP information about the neighboring devices received through all ports.

list: Displays the LLDP information about the neighboring devices in the form of a list.

system-name *system-name*: Displays the LLDP information about a specified neighboring device in the form of a list, where *system-name* indicates the system name of a neighboring device and is a string of 1 to 255 characters. If this keyword-argument combination is not specified, this command displays the LLDP information sent by all the neighboring devices in the form of a list.

Description

Use the **display lldp neighbor-information** command to display the LLDP information about the neighboring devices received on the local device. The LLDP information is sent as TLVs.

Examples

Display the LLDP information about the neighboring devices received through all the ports.

```
<Sysname> display lldp neighbor-information

LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
  Neighbor index   : 1
  Update time      : 0 days,0 hours,1 minutes,1 seconds
  Chassis type     : MAC address
  Chassis ID       : 000f-0055-0002
  Port ID type     : Interface name
  Port ID          : GigabitEthernet1/0/1
  Port description : GigabitEthernet1/0/1 Interface
  System name       : System
  System description : System
  System capabilities supported : Bridge,Router
  System capabilities enabled   : Bridge,Router

  Management address type         : ipv4
  Management address              : 192.168.1.55
  Management address interface type : IfIndex
  Management address interface ID   : Unknown
  Management address OID          : 0

  Port VLAN ID(PVID): 1

  Port and protocol VLAN ID(PPVID) : 1
```

```
  Port and protocol VLAN supported : Yes
  Port and protocol VLAN enabled   : No

  VLAN name of VLAN 1: VLAN 0001

  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             : Signal
  Port power classification : Class 0

  Link aggregation supported : Yes
  Link aggregation enabled   : No
  Aggregation port ID       : 0

  Maximum frame Size: 1536

LLDP neighbor-information of port 2[GigabitEthernet1/0/2]:
  Neighbor index   : 1
  Update time     : 0 days,0 hours,1 minutes,1 seconds
  Chassis type    : MAC address
  Chassis ID      : 000f-0055-0002
  Port ID type    : Interface name
  Port ID         : GigabitEthernet1/0/2
  Port description : GigabitEthernet1/0/2 Interface
  System name       : System
  System description : System
  System capabilities supported : Bridge,Router
  System capabilities enabled   : Bridge,Router

  Management address type         : ipv4
  Management address             : 127.0.0.1
  Management address interface type : IfIndex
  Management address interface ID   : Unknown
  Management address OID          : 0

  Port VLAN ID(PVID): 1

  Port and protocol VLAN ID(PPVID) : 1
  Port and protocol VLAN supported : Yes
  Port and protocol VLAN enabled   : No
```

```
  VLAN name of VLAN 1: VLAN 0001

  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              : Signal
  Port power classification : Class 0

  Link aggregation supported : Yes
  Link aggregation enabled   : No
  Aggregation port ID       : 0

  Maximum frame Size: 1536
```

Display the LLDP information about all the neighboring devices in the form of a list.

```
<Sysname> display lldp neighbor-information list

System Name          Local Interface Chassis ID    Port ID
System1             GE1/0/1        000f-e25d-ee91 GigabitEthernet1/0/5
System2             GE1/0/2        000f-e25d-ee92 GigabitEthernet1/0/6
System3             GE1/0/3        000f-e25d-ee93 GigabitEthernet1/0/7
```

Table 4-2 display lldp neighbor-information command output description

Field	Description
LLDP neighbor-information of port 1	LLDP information received through port 1
Neighbor index	Neighbor index
Update time	Time when the LLDP information about a neighboring device is latest updated.
Chassis type	Chassis information, which can be: • Chassis component • Interface alias • Port component • MAC address • Network address • Interface name • Locally assigned (indicating the local configuration)
Chassis ID	ID that identifies the LLDP sending device, which can be a MAC address, a network address, an interface or some other value depending on the chassis type.

Field	Description
Port ID type	Port information, which can be: • Interface alias • Port component • MAC address • Network Address • Interface name • Agent circuit ID • Locally assigned (indicating the local configuration)
Port ID	Port ID, the value of which depends on the port ID type
Port description	Port description
System name	System name of the neighboring device
System description	System description of the neighboring device
System capabilities supported	Capabilities supported on the neighboring device, which can be: • Repeater, indicating forwarding • Bridge, indicating switching • Router, indicating routing
System capabilities enabled	Capabilities currently enabled on the neighboring device, which can be: • Repeater, indicating forwarding is currently enabled. • Bridge, indicating switching is currently enabled. • Router, indicating routing is currently enabled.
Management address type	Management address type
Management address	Management address
Management address interface type	Type of the interface identified by the management address
Management address interface ID	Management address interface ID
Management address OID	Management address object ID
Port VLAN ID	Port VLAN ID
Port and protocol VLAN ID(PPVID)	Port protocol VLAN ID
Port and protocol VLAN supported	Indicates whether protocol VLAN is supported.
Port and protocol VLAN enabled	Indicates whether protocol VLAN is enabled.
VLAN name of VLAN 1	Name of VLAN 1
Auto-negotiation supported	Indicates whether auto-negotiation is supported.
Auto-negotiation enabled	State of auto-negotiation
OperMau	Current speed and duplex state
Power port class	PoE device type, which can be: • PSE: power sourcing equipment • PD: powered device
PSE power supported	Indicates whether or not the device can operate as a PSE.
PSE power enabled	Indicates whether or not the device is operating as a PSE.

Field	Description
PSE pairs control ability	Indicates whether or not the PSE-PD pair control is available.
Power pairs	PoE mode, which can be **Signal** (PoE via signal lines) or **Spare** (PoE via spare lines).
Port power classification	Port power classification of the PD, which can be the following: • Class0 • Class1 • Class2 • Class3 • Class4
Link aggregation supported	Indicates whether or not link aggregation is supported.
Link aggregation enabled	Indicates whether or not link aggregation is enabled.
Aggregation port ID	Aggregation group ID, which is 0 if link aggregation is not enabled.
Maximum frame Size	Maximum frame size supported
Location format	Location information format, which can be: • Invalid, indicating the format of the location information is invalid. • Coordinate-based LCI, indicating the location information is coordinate-based. • Civic Address LCI, indicating normal address information. • ECS ELIN, indicating a telephone for urgencies.
Location Information	Location information
PoE PSE power source	PSE power type, which can be: • Primary, indicating a primary power supply • Backup, indicating a backup power supply
PoE service type	PoE service type
Port PSE Priority	PoE power supply priority of PSE ports, which can be: • Unknown • Critical • High • Low
Port available power value	Available PoE power on PSE ports
Unknown basic TLV	Unknown basic TLV
TLV type	Unknown basic TLV type
TLV information	Information contained in the unknown basic TLV type
Unknown organizationally-defined TLV	Unknown organizationally specific TLV
TLV OUI	OUI of the unknown organizationally specific TLV
TLV subtype	Unknown organizationally specific TLV subtype
Index	Unknown organization index

Field	Description
TLV information	Information contained in unknown organizationally specific TLV
Local Interface	Local port that receives the LLDP information

display lldp statistics

Syntax

display lldp statistics [**global** | **interface** *interface-type interface-number*]

View

Any view

Default level

1: Monitor level

Parameters

global: Displays the global LLDP statistics.

interface *interface-type interface-number*: Specifies a port by its type and number.

Description

Use the **display lldp statistics** command to display the global LLDP statistics or the LLDP statistics of a port.

If no keyword/argument is specified, this command displays all the LLDP statistics.

Examples

Display all the LLDP statistics.

```
<Sysname> display lldp statistics
LLDP statistics global Information:
LLDP neighbor information last change time:0 days,0 hours,4 minutes,40 seconds
The number of LLDP neighbor information inserted : 1
The number of LLDP neighbor information deleted  : 1
The number of LLDP neighbor information dropped  : 0
The number of LLDP neighbor information aged out : 1
LLDP statistics Information of port 1 [GigabitEthernet1/0/1]:
The number of LLDP frames transmitted          : 0
The number of LLDP frames received             : 0
The number of LLDP frames discarded            : 0
The number of LLDP error frames               : 0
The number of LLDP TLVs discarded              : 0
The number of LLDP TLVs unrecognized           : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted           : 0
The number of CDP frames received              : 0
The number of CDP frames discarded             : 0
```

```
The number of CDP error frames                : 0
```

Table 4-3 display lldp statistics command output description

Field	Description
LLDP statistics global information	Global LLDP statistics
LLDP neighbor information last change time	Time the neighbor information is latest updated
The number of LLDP neighbor information inserted	Number of times of adding neighbor information
The number of LLDP neighbor information deleted	Number of times of removing neighbor information
The number of LLDP neighbor information dropped	Number of times of dropping neighbor information due to lack of available memory space
The number of LLDP neighbor information aged out	Number of the neighbor information entries that have aged out
LLDP statistics Information of port 1	LLDP statistics of port 1
The number of LLDP frames transmitted	Total number of the LLDP frames transmitted
The number of LLDP frames received	Total number of the LLDP frames received
The number of LLDP frames discarded	Total number of the LLDP frames dropped
The number of LLDP error frames	Total number of the LLDP error frames received
The number of LLDP TLVs discarded	Total number of the LLDP TLVs dropped
The number of LLDP TLVs unrecognized	Total number of the LLDP TLVs that cannot be recognized
The number of LLDP neighbor information aged out	Number of the LLDP neighbor information entries that have aged out
The number of CDP frames transmitted	Total number of the CDP frames transmitted
The number of CDP frames received	Total number of the CDP frames received
The number of CDP frames discarded	Total number of the CDP frames dropped
The number of CDP error frames	Total number of the CDP error frames received

display lldp status

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

Description

Use the **display lldp status** command to display the LLDP status of a port.

If no port is specified, this command displays the LLDP status of all the ports.

Examples

Display the LLDP status of all the ports.

```
<Sysname> display lldp status
Global status of LLDP: Enable
The current number of LLDP neighbors: 4
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days,0 hours,4 minutes,40 seconds
Transmit interval           : 30s
Hold multiplier             : 4
Reinit delay                : 2s
Transmit delay              : 2s
Trap interval               : 5s
Fast start times            : 3
Port 1 [GigabitEthernet1/0/1]:
Port status of LLDP         : Enable
Admin status                : Tx_Rx
Trap flag                   : No
Rolling interval            : 0s
Number of neighbors         : 5
Number of MED neighbors     : 2
Number of CDP neighbors     : 0
Number of sent optional TLV   : 12
Number of received unknown TLV : 5
```

Table 4-4 display lldp status command output description

Field	Description
Global status of LLDP	Indicating whether or not LLDP is globally enabled
The current number of LLDP neighbors	Total number of the LLDP neighbor devices
The current number of CDP neighbors	The current number of CDP neighbors
LLDP neighbor information last changed time	Time the neighbor information is latest updated
Transmit interval	Interval to send LLDPDU
Hold multiplier	TTL multiplier
Reinit delay	Initialization delay
Transmit delay	Delay period to send LLDPDUs
Trap interval	Interval to send traps
Fast start times	Number of the LLDPDUs to be sent successively when a new neighboring device is detected

Field	Description
Port 1	LLDP status of port 1
Port status of LLDP	Indicates whether or not LLDP is enabled on the port.
Admin status	LLDP mode of the port, which can be: • TxRx. A port in this mode sends and receives LLDPDUs. • Rx_Only. A port in this mode receives LLDPDUs only. • Tx_Only. A port in this mode sends LLDPDUs only. • Disable. A port in this mode does not send or receive LLDPDUs.
Trap Flag	Indicates whether or not trap is enabled.
Rolling interval	LLDP polling interval. A value of 0 indicates LLDP polling is disabled.
Number of neighbors	Number of the LLDP neighbors connecting to the port
Number of MED neighbors	Number of MED neighbors connecting to the port
Number of CDP neighbors	Number of the CDP neighbors connecting to the port
Number of sent optional TLV	Number of the optional TLVs contained in an LLDPDU sent through the port
Number of received unknown TLV	Number of the unknown TLVs contained in a received LLDPDU

display lldp tlv-config

Syntax

display lldp tlv-config [**interface** *interface-type interface-number*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

Description

Use the **display lldp tlv-config** command to display the advertisable TLVs of a port.

If no port is specified, this command displays the advertisable TLVs of each port.

Examples

Display the advertisable TLVs of port GigabitEthernet1/0/1.

```
<Sysname> display lldp tlv-config interface GigabitEthernet 1/0/1
LLDP tlv-config of port 1[GigabitEthernet1/0/1]:
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
IEEE 802.3 extend TLV:
MAC-Physic TLV                 YES      YES
Power via MDI TLV               YES      YES
Link Aggregation TLV            YES      YES
Maximum Frame Size TLV          YES      YES
LLDP-MED extend TLV:
Capabilities TLV               YES       YES
Network Policy TLV              YES       YES
Location Identification TLV      NO        NO
Extended Power via MDI TLV       YES       YES
Inventory TLV                  YES       YES
```

Table 4-5 display lldp tlv-config command output description

Field	Description
LLDP tlv-config of port 1	Advertisable TLVs of port 1
NAME	TLV type
STATUS	Indicates whether or not TLVs of a specific type are currently sent through a port
DEFAULT	Indicates whether or not TLVs of a specific type are sent through a port by default
Basic optional TLV	Basic TLVs, including: • Port description TLV • System name TLV • System description TLV • System capabilities TLV • Management address TLV
IEEE 802.1 extended TLV	IEEE 802.1 organizationally specific TLVs, including: • Port VLAN ID TLV • Port and protocol VLAN ID TLV • VLAN name TLV
IEEE 802.3 extended TLV	IEEE 802.3 organizationally specific TLVs, including: • MAC-Physic TLV • Power via MDI TLV • Link aggregation TLV • Maximum frame size TLV

Field	Description
LLDP-MED extend TLV	MED related LLDP TLVs, including: • Capabilities TLV • Network Policy TLV • Extended Power-via-MDI TLV • Location Identification TLV • Inventory TLV, which can be hardware revision TLV, firmware revision TLV, software revision TLV, serial number TLV, manufacturer name TLV, model name TLV, and asset id TLV.

lldp admin-status

Syntax

lldp admin-status { **disable** | **rx** | **tx** | **txrx** }

undo lldp admin-status

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

disable: Specifies the **Disable** mode. A port in this mode does not send or receive LLDPDUs.

rx: Specifies the **Rx** mode. A port in this mode receives LLDPDUs only.

tx: Specifies the **Tx** mode. A port in this mode sends LLDPDUs only.

txrx: Specifies the **TxRx** mode. A port in this mode sends and receives LLDPDUs.

Description

Use the **lldp admin-status** command to specify the LLDP operating mode for a port or all the ports in a port group.

Use the **undo lldp admin-status** command to restore the default LLDP operating mode.

The default LLDP operating mode is **TxRx**.

Examples

Configure the LLDP operating mode as **Rx** for GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp admin-status rx
```

lldp check-change-interval

Syntax

lldp check-change-interval *interval*

undo lldp check-change-interval

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

interval: LLDP polling interval to be set, in the range 1 to 30 (in seconds).

Description

Use the **lldp check-change-interval** command to enable LLDP polling and set the polling interval.

Use the **undo lldp check-change-interval** command to restore the default.

By default, LLDP polling is disabled.

With LLDP polling enabled, LLDP detects for local configuration changes periodically. A local configuration change triggers LLDPDU sending, through which neighboring devices can be informed of the configuration change timely.

Examples

Enable LLDP polling on GigabitEthernet1/0/1, setting the polling interval to 30 seconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp check-change-interval 30
```

lldp compliance admin-status cdp

Syntax

lldp compliance admin-status cdp { **disable** | **txrx** }

View

Ethernet interface view, port group view

Default Level

2: System level

Parameters

disable: Specifies the disable mode, where CDP-compatible LLDP neither receives nor transmits CDP packets.

txrx: Specifies the TxRx mode, where CDP-compatible LLDP can send and receive CDP packets.

Description

Use the **lldp compliance admin-status cdp** command to configure the operation mode of CDP-compatible LLDP on a port or port group.

By default, CDP-compatible LLDP operates in disable mode.

To have your device work with Cisco IP phones, you must enable CDP-compatible LLDP globally and then configure CDP-compatible LLDP to work in TxRx mode on the specified port(s).

Related commands: **lldp compliance cdp**.

Examples

Configure CDP-compatible LLDP to operate in TxRx mode on GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
```

lldp compliance cdp

Syntax

lldp compliance cdp

undo lldp compliance cdp

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **lldp compliance cdp** command to enable CDP compatibility globally.

Use the **undo lldp compliance cdp** command to restore the default.

By default, CDP compatibility is disabled globally.

Note that, as the maximum TTL allowed by CDP is 255 seconds, your TTL configuration, that is, the product of the TTL multiplier and the LLDPDU transmit interval, must be no more than 255 seconds for CDP-compatible LLDP to work properly with Cisco IP phones.

Related commands: **lldp hold-multiplier**, **lldp timer tx-interval**.

Examples

Enable LLDP to be compatible with CDP globally.

```
<Sysname> system-view
[Sysname] lldp compliance cdp
```

lldp enable

Syntax

lldp enable

undo lldp enable

View

System view, Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use the **lldp enable** command to enable LLDP.

Use the **undo lldp enable** command to disable LLDP.

By default, LLDP is disabled globally and enabled on a port.

Note that LLDP takes effect on a port only when it is enabled both globally and on the port.

Examples

Disable LLDP on GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo lldp enable
```

lldp encapsulation snap

Syntax

lldp encapsulation snap

undo lldp encapsulation [**snap**]

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use the **lldp encapsulation snap** command to configure the encapsulation format for LLDPDUs as SNAP on a port or a group of ports.

Use the **undo lldp encapsulation** command to restore the default encapsulation format for LLDPDUs.

By default, Ethernet II encapsulation applies.

Note

The command does not apply to LLDP-CDP packets, which use only SNAP encapsulation.

Examples

Configure the encapsulation format for LLDPDUs as SNAP on GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp encapsulation snap
```

lldp fast-count

Syntax

lldp fast-count *count*

undo lldp fast-count

View

System view

Default level

2: System level

Parameters

count: Number of the LLDPDUs to be sent successively when a new neighboring device is detected. This argument ranges from 1 to 10.

Description

Use the **lldp fast-count** command to set the number of the LLDPDUs to be sent successively when a new neighboring device is detected.

Use the **undo lldp fast-count** command to restore the default.

By default, the number is 3.

Examples

Configure to send four LLDP successively when a new neighboring device is detected.

```
<Sysname> system-view
[Sysname] lldp fast-count 4
```

lldp hold-multiplier

Syntax

lldp hold-multiplier *value*

undo lldp hold-multiplier

View

System view

Default level

2: System level

Parameters

value: TTL multiplier, in the range 2 to 10.

Description

Use the **lldp hold-multiplier** command to set the TTL multiplier.

Use the **undo lldp hold-multiplier command** to restore the default.

The TTL multiplier defaults to 4.

You can set the TTL of the local device information by configuring the TTL multiplier.

The TTL of the information about a device is determined by the following expression:

TTL multiplier × LLDPDU transmit interval

You can set the TTL of the local device information by configuring the TTL multiplier. Note that the TTL can be up to 65535 seconds. TTLs longer than it will be rounded off to 65535 seconds.

Related commands: **lldp timer tx-interval**.

Examples

Set the TTL multiplier to 6.

```
<Sysname> system-view
[Sysname] lldp hold-multiplier 6
```

lldp management-address-format string

Syntax

lldp management-address-format string

undo lldp management-address-format

View

Ethernet interface view, port group view

Default Level

2: System level

Parameters

None

Description

Use the **lldp management-address-format string** command to configure the encapsulation format of the management address as strings in TLVs.

Use the **undo lldp management-address-format** command to restore the default.

By default, the management address is encapsulated in the form of numbers in TLVs.

Examples

Configure GigabitEthernet1/0/1 to encapsulate the management address in the form of strings in management address TLVs.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp management-address-format string
```

lldp management-address-tlv

Syntax

lldp management-address-tlv [*ip-address*]

undo lldp management-address-tlv

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

ip-address: Management address to be set.

Description

Use the **lldp management-address-tlv** command to enable the management address sending. This command also sets the management address.

Use the **undo lldp management-address-tlv** command to disable management address sending.

By default, the management address is sent through LLDPDUs, and the management address is the primary IP address of the VLAN with the smallest VLAN ID among the VLANs whose packets are permitted on the port. If the primary IP address is not configured, the management address is 127.0.0.1.

Note that an LLDPDU carries only one management address. If you set the management address repeatedly, the latest one takes effect.

Examples

Set the management address to 192.6.0.1 for GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp management-address-tlv 192.6.0.1
```

lldp notification remote-change enable

Syntax

lldp notification remote-change enable

undo lldp notification remote-change enable

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

None

Description

Use the **lldp notification remote-change enable** command to enable trap for a port or all the ports in a port group.

Use the **undo lldp notification remote-change enable** command to restore the default.

By default, trap is disabled on a port.

Examples

Enable LLDP trap for GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp notification remote-change enable
```

lldp timer notification-interval

Syntax

lldp timer notification-interval *interval*

undo lldp timer notification-interval

View

System view

Default level

2: System level

Parameters

interval: Interval to send LLDP trap messages, in the range 5 to 3600 (in seconds).

Description

Use the **lldp timer notification-interval** command to set the interval to send LLDP trap messages.

Use the **undo lldp timer notification-interval** command to restore the default.

By default, the interval to send LLDP trap messages is 5 seconds.

Examples

Set the interval to send LLDP trap messages to 8 seconds.

```
<Sysname> system-view
```

```
[Sysname] lldp timer notification-interval 8
```

lldp timer reinit-delay

Syntax

lldp timer reinit-delay *delay*

undo lldp timer reinit-delay

View

System view

Default level

2: System level

Parameters

delay: Initialization delay period to be set, in the range 1 to 10 (in seconds).

Description

Use the **lldp timer reinit-delay** command to set the initialization delay period.

Use the **undo lldp timer reinit-delay** command to restore the default.

By default, the initialization delay period is 2 seconds.

Examples

Set the initialization delay period to 4 seconds.

```
<Sysname> system-view
[Sysname] lldp timer reinit-delay 4
```

lldp timer tx-delay

Syntax

lldp timer tx-delay *delay*

undo lldp timer tx-delay

View

System view

Default level

2: System level

Parameters

delay: Delay period to send LLDPDUs, in the range 1 to 8192 (in seconds).

Description

Use the **lldp timer tx-delay** command to set the delay period to send LLDPDUs.

Use the **undo lldp timer tx-delay** command to restore the default.

By default, the delay period to send LLDPDUs is 2 seconds.

Examples

Set the delay period to send LLDPDUs to 4 seconds.

```
<Sysname> system-view
[Sysname] lldp timer tx-delay 4
```

lldp timer tx-interval

Syntax

lldp timer tx-interval *interval*

undo lldp timer tx-interval

View

System view

Default level

2: System level

Parameters

interval: Interval to send LLDPDUs, in the range 5 to 32768 (in seconds).

Description

Use the **lldp timer tx-interval** command to set the interval to send LLDPDUs.

Use the **undo lldp timer tx-interval** command to restore the default.

By default, the interval to send LLDPDUs is 30 seconds.

To enable local device information to be updated on neighboring devices before being aged out, make sure the interval to send LLDPDUs is shorter than the TTL of the local device information.

Examples

Set the interval to send LLDPDUs to 20 seconds.

```
<Sysname> system-view
[Sysname] lldp timer tx-interval 20
```

lldp tlv-enable

Syntax

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } | **network-policy** | **power-over-ethernet** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** | **protocol-vlan-id** | **vlan-name** } | **dot3-tlv** { **all** |

link-aggregation | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **location-id** | **network-policy** | **power-over-ethernet** } }

View

Ethernet interface view, port group view

Default level

2: System level

Parameters

all: Sends all the basic LLDP TLVs, all the IEEE 802.1 organizationally specific LLDP TLVs, or all the IEEE 802.3 organizationally specific LLDP TLVs when the **all** keyword is specified for **basic-tlv**, **dot1-tlv**, or **dot3-tlv**; or sends all the MED related LLDP TLVs except location identification TLVs when the **all** keyword is specified for **med-tlv**.

basic-tlv: Sends basic LLDP TLVs.

port-description: Sends port description TLVs.

system-capability: Sends system capabilities TLVs.

system-description: Sends system description TLVs.

system-name: Sends system name TLVs.

dot1-tlv: Sends IEEE 802.1 organizationally specific LLDP TLVs.

port-vlan-id: Sends port VLAN ID TLVs.

protocol-vlan-id: Sends port and protocol VLAN ID TLVs.

vlan-name: Sends VLAN name TLVs.

vlan-id: ID of the VLAN in the TLVs (port and protocol VLAN ID TLVs or VLAN name TLVs) to be sent. This argument ranges from 1 to 4094 and defaults to the least protocol VLAN ID.

dot3-tlv: Sends IEEE 802.3 organizationally specific LLDP TLVs.

link-aggregation: Sends link aggregation group TLVs.

mac-physic: Sends MAC/PHY configuration/status TLVs.

max-frame-size: Sends maximum frame size TLVS.

power: Sends power via MDI TLVs.

med-tlv: Sends MED related LLDP TLVs.

capability: Sends LLDP-MED capabilities TLVs.

inventory: Sends hardware revision TLVs, firmware revision TLVs, software revision TLVs, serial number TLVs, manufacturer name TLVs, model name TLVs, and asset ID TLVs.

location-id: Sends location identification TLVS.

civic-address: Inserts the address information about the intermediate device in location identification TLVs .

device-type: Device type value. A value of 0 specifies DHCP server; a value of 1 specifies switch, and a value of 2 specifies LLDP-MED endpoint.

country-code: Country code, confirming to ISO 3166.

{ *ca-type ca-value* }&<1-10>: Configures address information, where *ca-type* represents the address information type, in the range 0 to 255, *ca-value* represents address information, a string of 1 to 250 characters, and &<1-10> indicates that you can enter up to ten such parameters.

elin-address: Inserts telephone numbers for urgencies in location identification TLVs.

tel-number: Telephone number for urgencies, a string of 10 to 25 characters.

network-policy: Sends network policy TLVs.

power-over-ethernet: Sends extended power-via-MDI TLVs.

Description

Use the **lldp tlv-enable** command to configure advertisable TLVs for a port or all the ports in a port group.

Use the **undo lldp tlv-enable** command to disable the sending of specific TLVs.

By default, all the TLVs except location identification TLVs are advertisable on a port.

Note that:

- To enable MED related LLDP TLV sending, you need to enable LLDP-MED capabilities TLV sending first. Conversely, to disable LLDP-MED capabilities TLV sending, you need to disable the sending of other MED related LLDP TLV.
- To disable MAC/PHY configuration/status TLV sending, you need to disable LLDP-MED capabilities TLV sending first.
- Enabling the sending of LLDP-MED capabilities TLVs also enables the sending of MAC/PHY configuration/status TLVs.
- You can specify to send multiple types of TLVs by executing the **lldp tlv-enable** command repeatedly.

Examples

Enable the sending of link aggregation group TLVs of the IEEE 802.3 organizationally specific TLVs on GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp tlv-enable dot3-tlv link-aggregation
```

5 VLAN Configuration Commands

VLAN Configuration Commands

description

Syntax

description *text*

undo description

View

VLAN view, VLAN interface view

Default Level

2: System level

Parameters

text: Case-sensitive string that describes the current VLAN or VLAN interface. Spaces can be included in the description.

- For a VLAN, this is a string of 1 to 32 characters.
- For a VLAN interface, this is a string of 1 to 80 characters.

Description

Use the **description** command to configure the description of the current VLAN or VLAN interface.

Use the **undo description** command to restore the default.

For a VLAN, the default description is the VLAN ID, for example, **VLAN 0001**; for a VLAN interface, the default description is the name of the interface, for example, **Vlan-interface 1 Interface**.

You can configure a description to describe the function or connection of a VLAN or VLAN interface for management sake.

Examples

Configure the description of VLAN 1 as **RESEARCH**.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] description RESEARCH
```

Configure the description of VLAN-interface 2 as **VLAN-INTERFACE-2**.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] description VLAN-INTERFACE-2
```

display interface vlan-interface

Syntax

display interface vlan-interface [*vlan-interface-id*]

View

Any view

Default Level

1: Monitor level

Parameters

vlan-interface-id: VLAN interface number, in the range of the numbers of existing VLANs on the device.

Description

Use the **display interface vlan-interface** command to display information about a specified or all VLAN interfaces if no interface is specified.

Related commands: **interface vlan-interface**.

Examples

Display the information of VLAN-interface 2.

```
<Sysname> display interface vlan-interface 2
Vlan-interface2 current state: DOWN
Line protocol current state: DOWN
Description: Vlan-interface2 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 001e-c16f-ae69
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 001e-c16f-ae69
```

Table 5-1 display interface vlan-interface command output description

Field	Description
Vlan-interface2 current state	The physical state of the VLAN interface, which can be one of the following: • Administratively DOWN: The administrative state of the VLAN interface is down because it has been manually shut down with the **shutdown** command. • DOWN: The administrative state of this VLAN interface is up, but its physical state is down. It indicates that the VLAN corresponding to this interface does not contain any port in the UP state (possibly because the ports are not well connected or the lines have failed). • UP: both the administrative state and the physical state of this VLAN interface are up.
Line protocol current state	The link layer protocol state of a VLAN interface, which can be one of the following: • DOWN: The protocol state of this VLAN interface is down, usually because no IP address is configured. • UP: The protocol state of this VLAN interface is up.

Field	Description
Description	The description string of a VLAN interface
The Maximum Transmit Unit	The MTU of a VLAN interface
Internet protocol processing :	IP packets processing ability. Disabled indicates that the interface is not configured with an IP address.
IP Packet Frame Type	IPv4 outgoing frame format
Hardware address	MAC address corresponding to a VLAN interface
IPv6 Packet Frame Type	IPv6 outgoing frame format

display vlan

Syntax

display vlan [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**]

View

Any view

Default Level

1: Monitor level

Parameters

vlan-id1: Displays the information of a VLAN specified by VLAN ID in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2*: Displays the information of a range of VLANs specified by a VLAN ID range. Note that *vlan-id2* must be equal to or greater than *vlan-id1*.

all: Displays all current VLAN information except for the reserved VLANs.

dynamic: Displays the number of dynamic VLANs and the ID of each dynamic VLAN. Dynamic VLANs refer to VLANs that are generated through GVRP or those distributed by a RADIUS server.

reserved: Displays information of the reserved VLANs. Protocol modules determine which VLANs are reserved VLANs according to function implementation, and reserved VLANs serve protocol modules. You cannot do any configuration on reserved VLANs.

static: Displays the number of static VLANs and the ID of each static VLAN. Static VLANs refer to VLANs manually created.

Description

Use the **display vlan** command to display VLAN information.

Related commands: **vlan**.

Examples

Display VLAN 2 information.

```
<Sysname> display vlan 2
VLAN ID: 2
 VLAN Type: static
 Route Interface: not configured
```

```
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged   Ports:
    GigabitEthernet1/0/11    GigabitEthernet1/0/12
 Untagged Ports: none
```

Display VLAN 3 information.

```
<Sysname> display vlan 3
 VLAN ID: 3
 VLAN Type: static
 Route Interface: configured
 IP Address: 1.1.1.1
 Subnet Mask: 255.255.255.0
 Description: VLAN 0003
 Name: VLAN 0003
 Tagged   Ports: none
 Untagged Ports: none
```

Table 5-2 display vlan command output description

Field	Description
VLAN ID	VLAN ID
VLAN Type	VLAN type (static or dynamic)
Route interface	Whether the VLAN interface is configured for the VLAN: not configured or configured
Description	VLAN description
Name	Name configured for the VLAN
IP Address	Primary IP address of the VLAN interface (available only on a VLAN interface configured with an IP address). You can use the **display interface vlan-interface** command in any view or the **display this** command in VLAN interface view to display its secondary IP address(es), if any.
Subnet Mask	Subnet mask of the primary IP address (available only on a VLAN interface configured with an IP address)
Tagged Ports	Ports through which packets of the VLAN are sent tagged
Untagged Ports	Ports through which packets of the VLAN are sent untagged

interface vlan-interface

Syntax

interface vlan-interface *vlan-interface-id*

undo interface vlan-interface *vlan-interface-id*

View

System view

Default Level

2: System level

Parameters

vlan-interface-id: VLAN interface number, in the range of 1 to 4094.

Description

Use the **interface vlan-interface** command to create a VLAN interface and enter its view or enter the view of an existing VLAN interface.

Before you can create the VLAN interface of a VLAN, create the VLAN first.

Use the **undo interface vlan-interface** command to remove the specified VLAN interface.

You can use the **ip address** command in VLAN interface view to configure an IP address for a VLAN interface to perform IP routing.

Related commands: **display interface Vlan-interface**.

Examples

Create VLAN-interface 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2]
```

ip address

Syntax

ip address *ip-address* { *mask* | *mask-length* } [**sub**]

undo ip address [*ip-address* { *mask* | *mask-length* } [**sub**]]

View

VLAN interface view

Default Level

2: System level

Parameters

ip-address: IP address to be assigned to the current VLAN interface, in dotted decimal format.

mask: Subnet mask in dotted decimal notation.

mask-length: Subnet mask length, the number of consecutive ones in the mask. The value range is 0 to 32.

sub: Indicates the address is a secondary IP address.

Description

Use the **ip address** command to assign an IP address and subnet mask to a VLAN interface.

Use the **undo ip address** command to remove the IP address and subnet mask for a VLAN interface.

By default, no IP address is assigned to any VLAN interface.

In general conditions, you need to assign only one IP address for a VLAN interface. For a VLAN to connect to multiple subnets, you need to assign multiple IP addresses for the VLAN interface. Among these IP addresses, one is primary and the others are secondary. On an Switch 4210G, you can assign up to ten IP addresses for a VLAN interface.

When configuring IP addresses for a VLAN interface, consider the following:

- You can assign only one primary IP address to an interface.
- Before removing the primary IP address, remove all secondary IP addresses.
- To remove all IP addresses, use the **undo ip address** command without any parameter.
- To remove the primary IP address, use the **undo ip address** *ip-address* { *mask* | *mask-length* } command.
- To remove a secondary IP address, use the **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command.

Related commands: **display ip interface** (*IP Address Commands* in the *IP Services Volume*).

Examples

Specify the IP address as 1.1.0.1, the subnet mask as 255.255.255.0 for VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 1.1.0.1 255.255.255.0
```

name

Syntax

name *text*

undo name

View

VLAN interface view

Default Level

2: System level

Parameters

text: VLAN name, a string of 1 to 32 characters. Spaces and special characters can be included in the name.

Description

Use the **name** command to configure a name for the current VLAN.

Use the **undo name** command to restore the default name of the VLAN.

The default name of a VLAN is its VLAN ID, **VLAN 0001** for example.

When 802.1X or MAC address authentication is configured on a switch, you can use a RADIUS server to issue VLAN configuration to ports that have passed the authentication. Some servers can send IDs or names of the issued VLANs to the switch. When there are a large number of VLANs, you can use VLAN names rather than VLAN IDs to better locate VLANs.

Examples

Configure the name of VLAN 2 as **test vlan**.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] name test vlan
```

shutdown

Syntax

shutdown

undo shutdown

View

VLAN interface view

Default Level

2: System level

Parameters

None

Description

Use the **shutdown** command to shut down a VLAN interface.

Use the **undo shutdown** command to bring up a VLAN interface.

By default, a VLAN interface is up except when all ports in the VLAN are down.

You can use the **undo shutdown** command to bring up a VLAN interface after configuring related parameters and protocols for the VLAN interface. When a VLAN interface fails, you can shut down the interface with the **shutdown** command and then bring it up with the **undo shutdown** command. In this way, the interface may resume.

The state of any Ethernet port in a VLAN is independent of the VLAN interface state.

Examples

Shut down VLAN interface 2 and then bring it up.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] shutdown
[Sysname-Vlan-interface2] undo shutdown
```

vlan

Syntax

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

View

System view

Default Level

2: System level

Parameters

vlan-id1, *vlan-id2*: VLAN ID, in the range 1 to 4094.

vlan-id1 **to** *vlan-id2*: Specifies a VLAN range. A VLAN ID is in the range 1 to 4094. Note that *vlan-id2* must be equal to or greater than *vlan-id1*.

all: Creates or removes all VLANs except reserved VLANs. The keyword is not supported when the maximum number of VLANs that can be created on a device is less than 4094.

Description

Use the **vlan** *vlan-id* command to create a VLAN and enter its view or enter the view of an existing VLAN.

Use the **vlan** *vlan-id1* **to** *vlan-id2* command to create a range of VLANs specified by *vlan-id1* **to** *vlan-id2*, except reserved VLANs.

Use the **undo vlan** command to remove the specified VLAN(s).

Note

- As the default VLAN, VLAN 1 cannot be created or removed.
- You cannot create/remove reserved VLANs reserved for specific functions.
- You cannot use the **undo vlan** command to directly remove reserved VLANs, voice VLANs, management VLANs, dynamic VLANs, VLANs configured with QoS policies, control VLANs configured for smart link, or remote probe VLANs configured for port mirroring. To remove these VLANs, you need to first remove related configurations.

Related commands: **display vlan**.

Examples

Enter VLAN 2 view.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2]
```

Create VLAN 4 through VLAN 100.

```
<Sysname> system-view
[Sysname] vlan 4 to 100
Please wait.............. Done.
```

Port-Based VLAN Configuration Commands

display port

Syntax

display port { **hybrid** | **trunk** }

View

Any view

Default Level

1: Monitor level

Parameters

hybrid: Displays hybrid ports.

trunk: Displays trunk ports.

Description

Use the **display port** command to display information about the hybrid or trunk ports on the device, including the port names, default VLAN IDs, and allowed VLAN IDs.

Examples

Display information about the hybrid ports in the system.

```
<Sysname> display port hybrid
Interface          PVID  VLAN passing
GE1/0/6            1     Tagged:  1002
                         Untagged:1-2, 5-50, 100, 200
```

Display information about the trunk ports in the system.

```
<Sysname> display port trunk
Interface          PVID  VLAN passing
GE1/0/1            100   2, 6-50, 100
GE1/0/11           1     1-2, 5-50, 100, 200, 1002
GE1/0/12           1     1-2, 5-50, 100, 200, 1002
```

Table 5-3 display port command output description

Field	Description
Interface	Port name
PVID	Default VLAN ID of the port
VLAN passing	VLANs whose packets are allowed to pass through the port.
Tagged	VLANs whose packets are required to pass through the port tagged.
Untagged	VLANs whose packets are required to pass through the port untagged.

port

Syntax

port *interface-list*

undo port *interface-list*

View

VLAN view

Default Level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet port list or Layer-2 aggregate interface list, in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 ports or port ranges.

Description

Use the **port** command to assign the specified access port(s) to the current VLAN.

Use the **undo port** command to remove the specified access port(s) from the current VLAN.

By default, all ports are in VLAN 1.

Note that:

- This command is only applicable on access ports.
- All ports are access ports by default. However, you can manually configure the port type. For more information, refer to **port link-type**.

Related commands: **display vlan**.

Examples

Assign GigabitEthernet 1/0/1 through GigabitEthernet 1/0/3 to VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

port access vlan

Syntax

port access vlan *vlan-id*

undo port access vlan

View

Ethernet interface view, port group view, Layer-2 aggregate interface view

Default Level

2: System level

Parameters

vlan-id: VLAN ID, in the range of 1 to 4094. Be sure that the VLAN specified by the VLAN ID already exists.

Description

Use the **port access vlan** command to assign the current access port(s) to the specified VLAN.

Use the **undo port access vlan** command to restore the default.

By default, all access ports belong to VLAN 1.

You can assign an access port to only one VLAN. When doing that, note the following:

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

Examples

Assign GigabitEthernet 1/0/1 to VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port access vlan 3
```

Assign Layer-2 aggregate interface **Bridge-aggregation 1** and its member ports to VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port access vlan 3
```

port hybrid pvid vlan

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

View

Ethernet interface view, port group view, Layer-2 aggregate interface view

Default Level

2: System level

Parameters

vlan-id: VLAN ID, in the range of 1 to 4094.

Description

Use the **port hybrid pvid vlan** command to configure the default VLAN ID of the hybrid port.

Use the **undo port hybrid pvid** command to restore the default.

By default, the default VLAN of a hybrid port is VLAN 1.

You can use a nonexistent VLAN as the default VLAN for a hybrid port. Removing the default VLAN of a hybrid port with the **undo vlan** command does not affect the setting of the default VLAN on the port.

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.
- The local and remote hybrid ports must use the same default VLAN ID for the traffic of the default VLAN to be transmitted properly.
- After configuring the default VLAN for a hybrid port, you must use the **port trunk permit vlan** command to configure the hybrid port to allow packets from the default VLAN to pass through, so that the port can forward packets from the default VLAN.

Related commands: **port link-type**, **port hybrid vlan**.

Examples

Configure VLAN 100 as the default VLAN of the hybrid port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid tagged 100
[Sysname-GigabitEthernet1/0/1] port hybrid pvid vlan 100
```

Configure VLAN 100 as the default VLAN of the hybrid Layer-2 aggregate interface **Bridge-aggregation 1**.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port hybrid pvid vlan 100
```

port hybrid vlan

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

View

Ethernet interface view, port group view, Layer-2 aggregate interface view

Default Level

2: System level

Parameters

vlan-id-list: VLANs that the hybrid ports will be assigned to. This argument is expressed in the format of [*vlan-id1* [**to** *vlan-id2*]]&<1-10>, where *vlan-id* ranges from 1 to 4094 and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges. Be sure that the specified VLANs already exist.

tagged: Configures the port(s) to send the packets of the specified VLAN(s) with the tags kept.

untagged: Configures the port to send the packets of the specified VLAN(s) with the tags removed.

Description

Use the **port hybrid vlan** command to assign the current hybrid port(s) to the specified VLAN(s).

Use the **undo port hybrid vlan** command to remove the current hybrid port(s) from the specified VLAN(s).

By default, a hybrid port only allows packets from VLAN 1 to pass through untagged.

A hybrid port can carry multiple VLANs. If you execute the **port hybrid vlan** command multiple times, the VLANs the hybrid port carries are the set of VLANs specified by *vlan-id-list* in each execution.

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

Related commands: **port link-type**.

Examples

Assign the hybrid port GigabitEthernet 1/0/1 to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100, and configure GigabitEthernet 1/0/1 to send packets of these VLANs with tags kept.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged
```

Assign hybrid ports in port group 2 to VLAN 2, and configure these hybrid ports to send packets of VLAN 2 with VLAN tags removed.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] port-group manual 2
[Sysname-port-group-manual-2] group-member gigabitethernet 1/0/1 to gigabitethernet 1/0/6
```

```
[Sysname-port-group-manual-2] port link-type hybrid
[Sysname-port-group-manual-2] port hybrid vlan 2 untagged
 Configuring GigabitEthernet1/0/1... Done.
 Configuring GigabitEthernet1/0/2... Done.
 Configuring GigabitEthernet1/0/3... Done.
 Configuring GigabitEthernet1/0/4... Done.
 Configuring GigabitEthernet1/0/5... Done.
 Configuring GigabitEthernet1/0/6... Done.
```

Assign the hybrid Layer-2 aggregate interface **Bridge-aggregation 1** and its member ports to VLAN 2, and configure them to send packets of VLAN 2 with tags removed.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 2 untagged
 Please wait... Done.
 Configuring GigabitEthernet1/0/2... Done.
 Configuring GigabitEthernet1/0/3... Done.
```

Note that GigabitEthernet1/0/2 and GigabitEthernet1/0/3 are the member ports of the aggregation group corresponding to Bridge-aggregation 1.

port link-type

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

View

Ethernet interface view, port group view, Layer-2 aggregate interface view

Default Level

2: System level

Parameters

access: Configures the link type of a port as access.

hybrid: Configures the link type of a port as hybrid.

trunk: Configures the link type of a port as trunk.

Description

Use the **port link-type** command to configure the link type of a port.

Use the **undo port link-type** command to restore the default link type of a port.

By default, any port is an access port.

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the

configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

Note

To change the link type of a port from trunk to hybrid or vice versa, you must set the link type to access first.

Examples

Configure GigabitEthernet 1/0/1 as a trunk port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
```

Configure all the ports in the manual port group **group1** as hybrid ports.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1] group-member gigabitethernet 1/0/2
[Sysname-port-group-manual-group1] group-member gigabitethernet 1/0/3
[Sysname-port-group-manual-group1] port link-type hybrid
```

Configure Layer-2 aggregate interface **Bridge-aggregation 1** and its member ports as hybrid ports.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
```

port trunk permit vlan

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

View

Ethernet interface view, port group view, Layer-2 aggregate interface view

Default Level

2: System level

Parameters

vlan-id-list: VLANs that the trunk port(s) will be assigned to. This argument is expressed in the format of [*vlan-id1* [**to** *vlan-id2*]]&<1-10>, where *vlan-id* ranges from 1 to 4094 and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.

all: Permits all VLANs to pass through the trunk port(s). On GVRP-enabled trunk ports, you must configure the **port trunk permit vlan all** command to ensure that the traffic of all dynamically registered VLANs can pass through. However, When GVRP is disabled on a port, you are discouraged to configure the command on the port. This is to prevent users of unauthorized VLANs from accessing restricted resources through the port.

Description

Use the **port trunk permit vlan** command to assign the current trunk port(s) to the specified VLAN(s).

Use the **undo port trunk permit vlan** command to remove the trunk port(s) from the specified VLANs.

By default, a trunk port allows only packets from VLAN 1 to pass through.

A trunk port can carry multiple VLANs. If you execute the **port trunk permit vlan** command multiple times, the VLANs the trunk port carries are the set of VLANs specified by *vlan-id-list* in each execution.

Note that on a trunk port, only traffic of the default VLAN can pass through untagged.

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

Related commands: **port link-type**.

Examples

Assign the trunk port GigabitEthernet 1/0/1 to VLAN 2, VLAN 4, and VLAN 50 through VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100
Please wait.......... Done.
```

Assign the trunk Layer-2 aggregate interface **Bridge-aggregation 1** to VLAN 2, assuming that **Bridge-aggregation 1** does not have member ports.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port trunk permit vlan 2
Please wait... Done.
```

Assign the trunk Layer-2 aggregate interface **Bridge-aggregation 1** to VLAN 13 and VLAN 15. Among the member ports of the aggregation group corresponding to **Bridge-aggregation 1**, GigabitEthernet 1/0/2 is an access port, and GigabitEthernet 1/0/3 is a trunk port.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port trunk permit vlan 13 15
 Please wait... Done.
 Error: Failed to configure on interface GigabitEthernet1/0/2! This port is not a Trunk port!
```

```
Configuring GigabitEthernet1/0/3... Done.
```

Among the output fields above, the message “Please wait... Done” indicates that the configuration on **Bridge-aggregation 1** succeeded; “Error: Failed to configure on interface GigabitEthernet1/0/2! This port is not a Trunk port!” indicates that the configuration failed on GigabitEthernet 1/0/2 because GigabitEthernet 1/0/2 was not a trunk port; “Configuring GigabitEthernet1/0/3... Done” indicates that the configuration on GigabitEthernet 1/0/3 succeeded.

port trunk pvid vlan

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

View

Ethernet interface view, port group view, Layer-2 aggregate interface view

Default Level

2: System level

Parameters

vlan-id: VLAN ID, in the range of 1 to 4094

Description

Use the **port trunk pvid vlan** command to configure the default VLAN ID for the trunk port.

Use the **undo port trunk pvid** command to restore the default.

By default, the default VLAN of a trunk port is VLAN 1.

You can use a nonexistent VLAN as the default VLAN for a trunk port. Removing the default VLAN of a trunk port with the **undo vlan** command does not affect the setting of the default VLAN on the port.

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.
- The local and remote trunk ports must use the same default VLAN ID for the traffic of the default VLAN to be transmitted properly.
- After configuring the default VLAN for a trunk port, you must use the **port trunk permit vlan** command to configure the trunk port to allow packets from the default VLAN to pass through, so that the port can forward packets from the default VLAN.

Related commands: **port link-type, port trunk permit vlan**.

Examples

Configure VLAN 100 as the default VLAN of the trunk port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk pvid vlan 100
```

Configure VLAN 100 as the default VLAN of the trunk Layer-2 aggregate interface **Bridge-aggregation 1**, assuming Bridge-aggregation 1 does not have member ports.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port trunk pvid vlan 100
```

Configure VLAN 100 as the default VLAN of the trunk Layer-2 aggregate interface **Bridge-aggregation 1**. Among the member ports of the aggregation group corresponding to **Bridge-aggregation 1**, GigabitEthernet 1/0/2 is an access port and GigabitEthernet 1/0/3 is a trunk port.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port trunk pvid vlan 100
 Error: Failed to configure on interface GigabitEthernet1/0/2! This port is not a Trunk port!
```

The output above shows that the configuration on Bridge-aggregation 1 and the member port GigabitEthernet 1/0/3 succeeded; the configuration on GigabitEthernet 1/0/2 failed because GigabitEthernet 1/0/2 was not a trunk port.

MAC Address-Based VLAN Configuration Commands

display mac-vlan

Syntax

display mac-vlan { **all** | **dynamic** | **mac-address** *mac-address* | **static** | **vlan** *vlan-id* }

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays all the MAC address-to-VLAN entries.

dynamic: Displays dynamically configured MAC address-to-VLAN entries.

mac-address *mac-address*: Displays the MAC address-to-VLAN entry containing the specified MAC address.

static: Displays the statically configured MAC address-to-VLAN entries.

vlan *vlan-id*: Displays the MAC address-to-VLAN entries associated with the specified VLAN.

Description

Use the **display mac-vlan** command to display the specified MAC address-to-VLAN entries.

If **mac-address** *mac-addr* is specified while **mask** is not specified, only the MAC address-to-VLAN entry containing the specified MAC address is displayed.

Examples

Display all the MAC address-to-VLAN entries.

```
<Sysname> display mac-vlan all
  The following MAC-VLAN address exist:
  S: Static   D: Dynamic
  MAC ADDR          MASK                VLAN ID   PRIO    STATE
  ------------------------------------------------------------------------
  0002-0001-0000    ffff-ffff-ffff        5        3      S&D

  Total MAC VLAN address count:1
```

Table 5-4 display mac-vlan command output description

Field	Description
S: Static	The character **S** stands for the MAC address-to-VLAN entries that are configured statically.
D: Dynamic	The character **D** stands for the MAC address-to-VLAN entries that are configured dynamically.
MAC ADDR	MAC address of a MAC address-to-VLAN entry
MASK	Mask of the MAC address of a MAC address-to-VLAN entry
VLAN ID	VLAN ID of a MAC address-to-VLAN entry
PRIO	802.1p priority corresponding to the MAC address of a MAC address-to-VLAN entry
STATE	The state of a MAC address-to-VLAN entry, which can be: • **S**, indicating that the MAC address-to-VLAN entry is configured statically. • **D**, indicating that the MAC address-to-VLAN entry is configured automatically through the authentication server • **S&D,** indicating that the MAC address-to-VLAN entry is configured both statically and dynamically

display mac-vlan interface

Syntax

display mac-vlan interface

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display mac-vlan interface** command to display all the ports with MAC address-based VLAN enabled.

Related commands: **mac-vlan enable**.

Examples

Display all the interfaces with MAC address-based VLAN enabled.

```
<Sysname> display mac-vlan interface
  MAC VLAN is enabled on following ports:
  ----------------------------------------
    GigabitEthernet1/0/1  GigabitEthernet1/0/2  GigabitEthernet1/0/3
```

mac-vlan enable

Syntax

mac-vlan enable

undo mac-vlan enable

View

Ethernet port view

Default Level

2: System level

Parameters

None

Description

Use the **mac-vlan enable** command to enable MAC address-based VLAN on a port.

Use the **undo mac-vlan enable** command to disable MAC address-based VLAN on a port.

By default, MAC address-based VLAN is disabled on a port.

Examples

Enable MAC address-based VLAN on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname–GigabitEthernet1/0/1] mac-vlan enable
```

mac-vlan mac-address

Syntax

mac-vlan mac-address *mac-address* **vlan** *vlan-id* [**priority** *pri*]

undo mac-vlan { **all** | **mac-address** *mac-address* | **vlan** *vlan-id* }

View

System view

Default Level

2: System level

Parameters

mac-address *mac-address*: Specifies a MAC address.

vlan *vlan-id*: Specifies a VLAN ID, in the range of 1 to 4094.

priority *pri*: Specifies the 802.1p priority value corresponding to the specified MAC address. This argument is in the range of 0 to 7.

all: Removes all the static MAC address-to-VLAN entries.

Description

Use the **mac-vlan mac-address** command to associate the specified VLAN and priority value with the specified MAC addresses.

Use the **undo mac-vlan** command to remove the association.

Examples

Associate a single MAC address 0-1-1 with VLAN 100 and 802.1p priority 7.

```
<Sysname> system-view
[Sysname] mac-vlan mac-address 0-1-1 vlan 100 priority 7
```

vlan precedence

Syntax

vlan precedence { **mac-vlan** | **ip-subnet-vlan** }

undo vlan precedence

View

Ethernet port view

Default Level

2: System level

Parameters

mac-vlan: Specifies to match VLANs based on MAC addresses preferentially.

ip-subnet-vlan: Specifies to match VLANs based on IP subnet settings preferentially.

Description

Use the **vlan precedence** command to set the order of VLAN matching.

Use the **undo vlan precedence** command to restore the default.

By default, VLANs are matched based on MAC addresses preferentially.

Note that this command only applies to VLANs based on a single MAC address and IP subnet-based VLANs. If both the MAC address-based VLAN function and the IP subnet-based VLAN function are

created on a port, MAC address-to-VLAN entries configured with the **mask** keyword specified are matched preferentially, and the left VLAN entries (VLAN entries based on a single MAC address and IP subnet-based VLANs) are matched as configured by the **vlan precedence** command.

Examples

Configure to match VLANs based on MAC addresses preferentially on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] vlan precedence mac-vlan
```

Protocol-Based VLAN Configuration Commands

display protocol-vlan interface

Syntax

display protocol-vlan interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] | **all** }

View

Any view

Default Level

2: System level

Parameters

interface-type interface-number1: Specifies an interface by its type and number.

interface-type interface-number1 **to** *interface-type interface-number2:* Specifies an interface range.

all: Displays information about protocol-based VLANs on all ports.

Description

Use the **display protocol-vlan interface** command to display information about protocol-based VLANs for the specified port(s).

Examples

Display protocol-based VLAN information on GigabitEthernet 1/0/1.

```
[Sysname] display protocol-vlan interface gigabitethernet 1/0/1
 Interface: GigabitEthernet1/0/1
   VLAN ID   Protocol Index     Protocol Type
 ============================================================
      3         0             ipv4
```

Table 5-5 display protocol-vlan interface command output description

Field	Description
Interface	Interface of which you want to view the information
VLAN ID	ID of the protocol-based VLAN bound with the port
Protocol Index	Protocol template index

Field	Description
Protocol Type	Protocol type specified by the protocol template

display protocol-vlan vlan

Syntax

display protocol-vlan vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

View

Any view

Default Level

2: System level

Parameters

vlan-id1: ID of the protocol-based VLAN for which information is to be displayed, in the range of 1 to 4094.

vlan-id1 **to** *vlan-id2*: Displays protocol-based VLAN information of a VLAN range from *vlan-id1* to *vlan-id2*. The *vlan-id2* argument specifies a protocol-based VLAN ID in the range of 1 to 4094, but you must ensure that its value is greater than or equal to that of *vlan-id1*.

all: Displays information about all protocol-based VLANs.

Description

Use the **display protocol-vlan vlan** command to display the protocols and protocol indexes configured on the specified VLAN(s).

Related commands: **display vlan**.

Examples

Display the protocols and protocol indexes configured on all protocol-based-VLANs.

```
<Sysname> display protocol-vlan vlan all
 VLAN ID:2
    Protocol Index     Protocol Type
 ======================================================
        0            ipv4
VLAN ID:3
    Protocol Index     Protocol Type
 ======================================================
        0            ipv4
        1            ipx snap
```

Refer to Table 5-5 for description of the output.

port hybrid protocol-vlan

Syntax

port hybrid protocol-vlan vlan *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }

undo port hybrid protocol-vlan { **vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** } | **all** }

View

Ethernet interface view, port group view, Layer-2 aggregate interface view

Default Level

2: System level

Parameters

vlan *vlan-id*: Specifies a VLAN ID, in the range 1 to 4094.

protocol-index: Protocol index, ranging from 0 to 15, specified by the users or assigned by the system automatically when the protocol-based VLAN is created. You can use the **display protocol-vlan vlan all** command to display the protocol indexes.

to *protocol-end*: Specifies the end protocol index, ranging from 0 to 15. The *protocol-end* argument must be greater than or equal to the beginning protocol index.

all: Specifies all protocols bound with *vlan-id*.

Description

Use the **port hybrid protocol-vlan vlan** command to associate the hybrid port(s) with a protocol-based VLAN.

Use the **undo port hybrid protocol-vlan** command to remove the association.

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

Before issuing this command, make sure that you have made the following configurations:

- Create a VLAN and associate it with specified protocols.
- Configure the link type as hybrid.
- Configure the port to allow the protocol-based VLAN to pass through.

Related commands: **display protocol-vlan interface**.

Examples

Associate the hybrid port GigabitEthernet 1/0/1 with protocol 0 (IPv4) in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] protocol-vlan ipv4
```

```
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 untagged
 Please wait... Done
[Sysname-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 2 0
```

Associate the hybrid Layer-2 aggregate interface **Bridge-aggregation 1** with protocol 0 in VLAN 2, assuming that **Bridge-aggregation 1** does not have member ports.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-Vlan2] protocol-vlan ipv4
[Sysname-Vlan2] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 2 untagged
 Please wait... Done
[Sysname-Bridge-Aggregation1] port hybrid protocol-vlan vlan 2 0
```

Associate the hybrid Layer-2 aggregate interface **Bridge-aggregation 1** with protocol 0 in VLAN 2. Among the member ports of the aggregation group corresponding to **Bridge-aggregation 1**, GigabitEthernet 1/0/2 is an access port and GigabitEthernet 1/0/3 is a trunk port.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-Vlan2] protocol-vlan at
[Sysname-Vlan2] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation2] port link-type access
 Please wait... Done.
 Configuring GigabitEthernet1/0/2... Done.
 Configuring GigabitEthernet1/0/3..................................... Done.
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 2 untagged
 Please wait... Done.
 Configuring GigabitEthernet1/0/2... Done.
 Configuring GigabitEthernet1/0/3... Done.
[Sysname-Bridge-Aggregation1] port hybrid protocol-vlan vlan 2 0
```

protocol-vlan

Syntax

protocol-vlan [*protocol-index*] { **at** | **ipv4 | ipv6** | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii etype** *etype-id* | **llc** { **dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id* } | **snap etype** *etype-id* } }

undo protocol-vlan { *protocol-index* [**to** *protocol-end*] | **all** }

View

VLAN view

Default Level

2: System level

Parameters

at: Specifies the AppleTalk based VLAN.

ipv4: Specifies the IPv4 based VLAN.

ipv6: Specifies the IPv6 based VLAN.

ipx: Specifies the IPX based VLAN. The keywords **ethernetii**, **llc**, **raw**, and **snap** are encapsulation formats for IPX.

mode: Configures a user-defined protocol template for the VLAN, which could also have four encapsulation formats, namely, **ethernetii**, **llc**, **raw**, and **snap**.

ethernetii etype *etype-id*: Specifies to match Ethernet II encapsulation format and the corresponding protocol type values. The *etype-id* argument is the protocol type ID of inbound packets, in the range 0x0600 to 0xffff (excluding 0x0800, 0x809b, 0x8137, and 0x86dd).

llc: Specifies to match the **llc** encapsulation format.

dsap *dsap-id*: Specifies the destination service access point, in the range of 00 to 0xff.

ssap *ssap-id*: Specifies the source service access point, in the range of 00 to 0xff.

snap etype *etype-id*: Specifies to match SNAP encapsulation format and the corresponding protocol type values. The *etype-id* argument is the Ethernet type of inbound packets, in the range 0x0600 to 0xffff (excluding **ipx snap** under the **snap** encapsulation format).

protocol-index: Protocol index, ranging from 0 to 15, which specifies the protocol template to be bound with the current VLAN. System will automatically assign an index if this parameter is not specified.

to *protocol-end*: Specifies the end protocol index, ranging from 0 to 15. The *protocol-end* argument must be greater than or equal to the *protocol-index* argument.

all: Specifies to remove all the protocols bound with the current VLAN.

Caution

- Do not configure both the *dsap-id* and *ssap-id* arguments in the **protocol-vlan** command as 0xe0 or 0xff when configuring the user-defined template for **llc** encapsulation. Otherwise, the encapsulation format of the matching packets will be the same as that of the **ipx llc** or **ipx raw** packets respectively. When either of the *dsap-id* and *ssap-id* arguments is configured, the system assigns **aa** to the other argument.
- When you use the **mode** keyword to configure a user-defined protocol template, do not set *etype-id* in **ethernetii etype** *etype-id* to 0x0800, 0x8137, 0x809b, or 0x86dd. Otherwise, the encapsulation format of the matching packets will be the same as that of the IPv4, IPX, AppleTalk, and IPv6 packets respectively.

Description

Use the **protocol-vlan** command to configure the VLAN as a protocol based VLAN and configure the protocol template for the VLAN.

Use the **undo protocol-vlan** command to remove the configured protocol template.

By default, no VLAN is bound with any protocol template.

Related commands: **display protocol-vlan vlan**.

Note

Do not configure a VLAN as both a protocol-based VLAN and a voice VLAN.

Examples

Configure VLAN 3 as an IPv4 based VLAN.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] protocol-vlan ipv4
```

Caution

Because IP depends on ARP for address resolution in Ethernet, you are recommended to configure the IP and ARP templates in the same VLAN and associate them with the same port to prevent communication failure.

Create an ARP protocol template for VLAN 3 (ARP code is 0x0806) to make VLAN 3 transmit ARP packets.

- To use Ethernet encapsulation, use the command:

```
[Sysname-vlan3] protocol-vlan mode ethernetii etype 0806
```

- To use 802.3 encapsulation, use the command:

```
[Sysname-vlan3] protocol-vlan mode snap etype 0806
```

IP Subnet-Based VLAN Configuration Commands

display ip-subnet-vlan interface

Syntax

display ip-subnet-vlan interface { *interface-list* | **all** }

View

Any view

Default Level

2: System level

Parameters

interface-list: Specifies an Ethernet port list in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where *interface-type interface-number* represents the port type and port number and &<1-10> indicates that you can specify up to 10 ports or port ranges.

all: Displays IP subnet-based VLAN information about all the ports with IP subnet-based VLAN configured.

Description

Use the **display ip-subnet-vlan interface** command to display IP subnet-based VLANs and IP subnet indexes on the specified port(s).

Examples

Display IP subnet-based VLANs and IP subnet indexes on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname]display ip-subnet-vlan interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
  VLAN ID   Subnet-Index    IP ADDRESS       NET MASK
  ========================================================
    3          0           192.168.1.0    255.255.255.0
```

Table 5-6 display ip-subnet-vlan interface command output description

Field	Description
Interface	Interface of which you want to view the information
VLAN ID	VLAN ID
Subnet-Index	Index of the IP subnet
IP ADDRESS	IP address of the subnet (either an IP address or a network address)
NET MASK	Mask of the IP subnet

display ip-subnet-vlan vlan

Syntax

display ip-subnet-vlan vlan { *vlan-id* [**to** *vlan-id*] | **all** }

View

Any view

Default Level

2: System level

Parameters

vlan-id: VLAN ID, in the range 1 to 4094.

to: Specifies a VLAN ID range. The argument after this keyword must be greater than or equal to the one before this keyword.

all: Specifies all the VLANs.

Description

Use the **display ip-subnet-vlan vlan** command to display the IP subnet information and IP subnet indexes on the specified VLAN(s).

Related commands: **display vlan**.

Examples

Display the IP subnet information of all VLANs.

```
<Sysname> display ip-subnet-vlan vlan all
VLAN ID:  3
 Subnet Index     IP Address     Subnet Mask
 ================================================
      0         192.168.1.0    255.255.255.0
```

Table 5-7 display ip-subnet-vlan vlan command output description

Field	Description
VLAN ID	VLAN ID
Subnet Index	IP subnet index
IP Address	IP address of the subnet (can be an IP address or a network address)
Subnet Mask	Mask of the IP subnet

ip-subnet-vlan

Syntax

ip-subnet-vlan [*ip-subnet-index*] **ip** *ip-address* [*mask*]

undo ip-subnet-vlan { *ip-subnet-index* [**to** *ip-subnet-end*] | **all** }

View

VLAN view

Default Level

2: System level

Parameters

ip-subnet-index: Beginning IP subnet Index, in the range of 0 to 11. This value can be configured by users, or automatically numbered by system based on the order in which the IP subnets or IP addresses are associated with the VLAN.

ip *ip-address* [*mask*]: Specifies the source IP address or network address based on which the subnet-based VLANs are classified, in dotted decimal notation. The *mask* argument is the subnet mask of the source IP address or network address, in dotted decimal notation with a default value of 255.255.255.0.

to: Specifies an IP subnet index range.

ip-subnet-end: End IP subnet index, in the range of 0 to 11. This argument must be greater than or equal to the beginning IP subnet index.

all: Removes all the associations between VLANs and IP subnets or IP addresses.

Description

Use the **ip-subnet-vlan** command to associate the current VLAN with a specified IP subnet or IP address.

Use the **undo ip-subnet-vlan** command to remove the association.

Note that the IP subnet or IP address cannot be a multicast network segment or a multicast address.

Related commands: **display ip-subnet-vlan vlan**.

Examples

Configure VLAN 3 as an IP subnet-based VLAN and associate it with the 192.168.1.0/24 network segment.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
```

port hybrid ip-subnet-vlan vlan

Syntax

port hybrid ip-subnet-vlan vlan *vlan-id*

undo port hybrid ip-subnet-vlan { **vlan** *vlan-id* | **all** }

View

Ethernet interface view, port group view, Layer-2 aggregate interface view

Default Level

2: System level

Parameters

vlan-id: VLAN ID, in the range of 1 to 4094.

all: Specifies all VLANs.

Description

Use the **port hybrid ip-subnet-vlan vlan** command to associate the current Ethernet port with the specified IP subnet-based VLAN.

Use the **undo port hybrid ip-subnet-vlan vlan** command to remove the association.

On an Ethernet port associated with an IP subnet-based VLAN, if the source IP address of a received untagged packet belongs to the corresponding IP subnet, the port tags the packet with the corresponding VLAN tag.

- In port group view, this command applies to all ports in the port group. For information about port groups, refer to *Ethernet Interface Configuration* in the *Access Volume*.
- In Layer-2 aggregate interface view, this command applies to the Layer-2 aggregate interface and all its member ports. After you perform the configuration, the system starts applying the

configuration to the aggregate interface and its aggregation member ports. If the system fails to do that on the aggregate interface, it stops applying the configuration to the aggregation member ports. If it fails to do that on an aggregation member port, it simply skips the port and moves to the next port. For information about Layer-2 aggregate interfaces, refer to *Link Aggregation Configuration* in the *Access Volume*.

Currently, only hybrid ports support this feature. Before issuing this command, make sure that you have assigned the port to the IP subnet-based VLAN to be associated with.

Related commands: **display ip-subnet-vlan interface**.

Examples

Associate GigabitEthernet 1/0/1 with the IP subnet-based VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
[Sysname-vlan3] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 3 untagged
 Please wait... Done.
[Sysname-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 3
```

Associate the hybrid Layer-2 aggregate interface **Bridge-aggregation 1** with the IP subnet-based VLAN 3 (assuming that **Bridge-aggregation 1** does not have member ports).

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
[Sysname-vlan3] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 3 untagged
 Please wait... Done
[Sysname-Bridge-Aggregation1] port hybrid ip-subnet-vlan vlan 3
```

Associate the hybrid Layer-2 aggregate interface **Bridge-aggregation 1** with the IP subnet-based VLAN 3. Among the member ports of the aggregation group corresponding to **Bridge-aggregation 1**, GigabitEthernet 1/0/2 is an access port and GigabitEthernet 1/0/3 is a trunk port.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] ip-subnet-vlan ip 192.168.1.0 255.255.255.0
[Sysname-vlan3] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] port link-type access
 Please wait... Done.
 Configuring GigabitEthernet1/0/2... Done.
 Configuring GigabitEthernet1/0/3..................................... Done.
[Sysname-Bridge-Aggregation1] port link-type hybrid
[Sysname-Bridge-Aggregation1] port hybrid vlan 3 untagged
Please wait... Done.
```

```
 Configuring GigabitEthernet1/0/2... Done.
 Configuring GigabitEthernet1/0/3... Done.
[Sysname-Bridge-Aggregation1] port hybrid ip-subnet-vlan vlan 3
```

6 Isolate-User-VLAN Configuration Commands

Isolate-User-VLAN Configuration Commands

display isolate-user-vlan

Syntax

display isolate-user-vlan [*isolate-user-vlan-id*]

View

Any view

Default Level

1: Monitor level

Parameters

isolate-user-vlan-id: Isolate-user-VLAN ID, in the range of 1 to 4094.

Description

Use the **display isolate-user-vlan** command to display the mapping between an isolate-user-vlan and secondary VLAN(s), and the information of these VLANs.

Related commands: **isolate-user-vlan**, **isolate-user-vlan enable**.

Examples

Display the mapping between an isolate-user-vlan and secondary VLANs.

```
<Sysname> display isolate-user-vlan
 Isolate-user-VLAN VLAN ID : 2
 Secondary VLAN ID : 3 4

 VLAN ID: 2
 VLAN Type: static
 Isolate-user-VLAN type : isolate-user-VLAN
 Route Interface: configured
 IP Address: 1.1.1.1
 Subnet Mask: 255.255.255.0
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged   Ports: none
 Untagged Ports:
   GigabitEthernet1/0/2          GigabitEthernet1/0/3          GigabitEthernet1/0/4

 VLAN ID: 3
 VLAN Type: static
```

```
Isolate-user-VLAN type : secondary
Route Interface: configured
IP Address: 2.2.2.2
Subnet Mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged   Ports: none
Untagged Ports:
   GigabitEthernet1/0/2          GigabitEthernet1/0/3

VLAN ID: 4
VLAN Type: static
Isolate-user-VLAN type : secondary
Route Interface: not configured
Description: VLAN 0004
Name: VLAN 0004
Tagged   Ports: none
Untagged Ports:
   GigabitEthernet1/0/2          GigabitEthernet1/0/4
```

Table 6-1 display isolate-user-vlan command output description

Field	Description
Isolate-user-VLAN VLAN ID	Isolate-user-VLAN ID
Secondary VLAN ID	Secondary VLAN ID
VLAN ID	VLAN ID
VLAN Type	VLAN type, static or dynamic
Isolate-user-VLAN type	Current VLAN type, isolate-user-VLAN or secondary VLAN
Route Interface	Whether a VLAN interface is configured for the VLAN
IP Address	IP address of the VLAN interface, if configured. This field is not displayed if no IP address is configured for the VLAN interface.
Subnet Mask	Subnet mask of the VLAN interface, if configured. This field is not displayed if no mask is configured for the VLAN interface.
Description	VLAN description
Name	Name configured for the VLAN
Tagged Ports	Ports through which packets of this VLAN are sent tagged
Untagged Ports	Ports through which packets of this VLAN are sent untagged

isolate-user-vlan

Syntax

isolate-user-vlan *isolate-user-vlan-id* **secondary** *secondary-vlan-id* [**to** *secondary-vlan-id*]

undo isolate-user-vlan *isolate-user-vlan-id* [**secondary** *secondary-vlan-id* [**to** *secondary-vlan-id*]

View

System view

Default Level

2: System level

Parameters

isolate-user-vlan-id: Isolate-user-VLAN ID, in the range 1 to 4094.

secondary *secondary-vlan-id* [**to** *secondary-vlan-id*]: Specifies a secondary VLAN ID or a secondary VLAN ID range. The *secondary-vlan-id* argument is a secondary VLAN ID, in the range 1 to 4094.

Description

Use the **isolate-user-vlan** command to associate an isolate-user-VLAN with the specified secondary VLAN(s).

Use the **undo isolate-user-vlan** command to remove the association.

By default, an isolate-user-VLAN is not associated with any secondary VLAN. .

Note that:

- To use the **isolate-user-vlan** command, each of the isolate-user-VLAN and the secondary VLAN(s) must have at least one port which allows its isolate-user-VLAN or secondary VLAN to pass through, and the default VLAN of the port must be its isolate-user-VLAN or secondary VLAN.
- The **undo isolate-user-vlan** command without the **secondary** *secondary-vlan-id* parameter specified removes the association between the specified isolate-user-VLAN and all its secondary VLANs, while the **undo isolate-user-vlan** command with the **secondary** *secondary-vlan-id* parameter specified only removes the association between the specified isolate-user-VLAN and the specified secondary VLANs.

Note

After associating an isolate-user-VLAN with the specified secondary VLANs, you cannot add/remove a port to/from each involved VLAN or remove each involved VLAN. To do that, you must cancel the association first.

Related commands: **display isolate-user-vlan**.

Examples

Associate isolate-user-VLAN 2 with the secondary VLANs VLAN 3 and VLAN 4.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] isolate-user-vlan enable
[Sysname-vlan2] port gigabitethernet 1/0/2
[Sysname-vlan2] vlan 3
[Sysname-vlan3] port gigabitethernet 1/0/3
[Sysname-vlan3] vlan 4
```

```
[Sysname-vlan4] port gigabitethernet 1/0/4
[Sysname-vlan4] quit
[Sysname] isolate-user-vlan 2 secondary 3 to 4
```

isolate-user-vlan enable

Syntax

isolate-user-vlan enable

undo isolate-user-vlan enable

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **isolate-user-vlan enable** command to configure the current VLAN as an isolate-user-VLAN.

Use the **undo isolate-user-vlan enable** command to remove the isolate-user-VLAN configuration for the current VLAN.

By default, no VLAN is an isolate-user-VLAN.

An isolate-user-VLAN may include multiple ports, including the one connected to the upstream device.

Related commands: **display isolate-user-vlan**.

Examples

Configure VLAN 5 as an isolate-user-VLAN.

```
<Sysname> system-view
[Sysname] vlan 5
[Sysname-vlan5] isolate-user-vlan enable
```

7 Voice VLAN Configuration Commands

Voice VLAN Configuration Commands

display voice vlan oui

Syntax

display voice vlan oui

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display voice vlan oui** command to display the currently supported organizationally unique identifier (OUI) addresses, the OUI address masks, and the description strings.

Related commands: **voice vlan mac-address**.

 **Note**

In general, as the first 24 bits of a MAC address (in binary format), an OUI address is a globally unique identifier assigned to a vendor by IEEE. OUI addresses mentioned in this document, however, are different from those in common sense. OUI addresses in this document are used to determine whether a received packet is a voice packet. They are the results of the AND operation of the two arguments *mac-address* and *oui-mask* in the **voice vlan mac-address** command.

Examples

Display the currently supported OUI addresses.

```
<Sysname> display voice vlan oui
Oui Address    Mask          Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
```

```
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3com phone
```

Table 7-1 display voice vlan oui command output description

Field	Description
Oui Address	OUI addresses supported
Mask	Masks of the OUI addresses supported
Description	Description strings of the OUI addresses supported

display voice vlan state

Syntax

display voice vlan state

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display voice vlan state** command to display voice VLAN configuration.

Related commands: **voice vlan** *vlan-id* **enable**, **voice vlan enable**.

Examples

Display voice VLAN configurations.

```
<Sysname> display voice vlan state
Maximum of Voice VLANs: 8
 Current Voice VLANs: 2
 Voice VLAN security mode: Security
 Voice VLAN aging time: 1440 minutes
 Voice VLAN enabled port and its mode:
 PORT                    VLAN       MODE
 ---------------------------------------------
 GigabitEthernet1/0/1       2         AUTO
 GigabitEthernet1/0/2       3         AUTO
```

Table 7-2 display voice vlan state command output description

Field	Description
Maximum of Voice VLANs	Maximum number of voice VLANs supported by the system
Current Voice VLANs	Number of existing voice VLANs
Voice VLAN security mode	Security mode of the voice VLAN: Security for security mode; Normal for normal mode
Voice VLAN aging time	Aging time of the voice VLAN
Voice VLAN enabled port and its mode	Voice VLAN-enabled port and its voice VLAN assignment mode
PORT	Voice VLAN-enabled port name
VLAN	ID of the voice VLAN enabled on the port
MODE	Voice VLAN assignment mode of the port: manual or automatic.

voice vlan aging

Syntax

voice vlan aging *minutes*

undo voice vlan aging

View

System view

Default Level

2: System level

Parameters

minutes: Voice VLAN aging time, in the range 5 to 43200 minutes.

Description

Use the **voice vlan aging** command to configure the voice VLAN aging time.

Use the **undo voice vlan aging** command to restore the default.

By default, the voice VLAN aging time is 1440 minutes.

When a port in automatic voice VLAN assignment mode receives a voice packet, the system decides whether to assign the port to the voice VLAN based on the source MAC address of the voice packet. Upon assigning the port to the voice VLAN, the system starts the aging timer. If no voice packets are received on the port until the aging time expires, the system automatically removes the port from the voice VLAN. This aging time only applies to the ports in automatic voice VLAN assignment mode.

Related commands: **display voice vlan state**.

Examples

Configure the voice VLAN aging time as 100 minutes.

```
<Sysname> system-view
```

```
[Sysname] voice vlan aging 100
```

voice vlan enable

Syntax

voice vlan *vlan-id* **enable**

undo voice vlan enable

View

Ethernet interface view

Default Level

2: System level

Parameters

vlan-id: VLAN to be configured as the voice VLAN for the current port.

Description

Use the **voice vlan enable** command to enable the voice VLAN feature and configure a VLAN as the voice VLAN for the current Ethernet port.

Use the **undo voice vlan enable** command to disable the voice VLAN feature on an Ethernet port.

By default, the voice VLAN feature is disabled on ports.

You can enable the voice VLAN feature on a hybrid or trunk port operating in automatic voice VLAN assignment mode but not on an access port operating in automatic voice VLAN assignment mode.

You can configure different voice VLANs for different ports. An Switch 4210G ts up to eight voice VLANs globally.

Examples

Enable the voice VLAN feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] voice vlan 2 enable
```

voice vlan mac-address

Syntax

voice vlan mac-address *mac-address* **mask** *oui-mask* [**description** *text*]

undo voice vlan mac-address *oui*

View

System view

Default Level

2: System level

Parameters

mac-address: Source MAC address of voice traffic, in the format of H-H-H, such as 1234-1234-1234.

mask *oui-mask*: Specifies the valid length of the OUI address by a mask in the format of H-H-H, formed by consecutive **F**s and **0**s, for example, FFFF-0000-0000. To filter the voice device of a specific vendor, set the mask to FFFF-FF00-0000.

description *text*: Specifies a string that describes the OUI address. The string is of 1 to 30 case-sensitive characters.

oui: Specifies the OUI address to be removed, in the format of H-H-H, such as 1234-1200-0000. An OUI address is the logic AND result of *mac-address* and *oui-mask.* An OUI address cannot be a broadcast address, a multicast address, or an address of all **0**s or all **F**s. You can use the **display voice vlan oui** command to display the OUI addresses supported currently.

Description

Use the **voice vlan mac-address** command to add a recognizable OUI address.

Use the **undo voice vlan mac-address** command to remove a recognizable OUI address.

The system supports up to 16 OUI addresses.

By default, the system is configured with the default OUI addresses, as illustrated in Table 7-3. You can remove the default OUI addresses and then add recognizable OUI addresses manually.

Table 7-3 Default OUI addresses

Number	OUI	Description
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	00d0-1e00-0000	Pingtel phone
5	0060-b900-0000	Philips/NEC phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3com phone

Related commands: **display voice vlan oui**.

Examples

Add a recognizable OUI address 1234-1200-0000 by specifying the MAC address as 1234-1234-1234 and the mask as fff-ff00-0000, and configure its description string as PhoneA.

```
<Sysname> system-view
[Sysname] voice vlan mac-address 1234-1234-1234 mask ffff-ff00-0000 description PhoneA
```

Display the supported OUI addresses to verify the above configuration.

```
<Sysname> display voice vlan oui
Oui Address    Mask          Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
```

```
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3com phone
1234-1200-0000  ffff-ff00-0000  PhoneA
```

Remove the OUI address 1234-1200-0000.

```
<Sysname> system-view
[Sysname] undo voice vlan mac-address 1234-1200-0000
```

voice vlan mode auto

Syntax

voice vlan mode auto

undo voice vlan mode auto

View

Ethernet interface view

Default Level

2: System level

Parameters

None

Description

Use the **voice vlan mode auto** command to configure the current port to operate in automatic voice VLAN assignment mode.

Use the **undo voice vlan mode auto** command to configure the current port to operate in manual voice VLAN assignment mode.

By default, a port operates in automatic voice VLAN assignment mode.

The voice VLAN modes of different ports are independent of one another.

To make voice VLAN take effect on a port which is enabled with voice VLAN and operates in manual voice VLAN assignment mode, you need to assign the port to the voice VLAN manually.

Examples

Configure GigabitEthernet 1/0/1 to operate in manual voice VLAN assignment mode.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo voice vlan mode auto
```

voice vlan security enable

Syntax

voice vlan security enable

undo voice vlan security enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **voice vlan security enable** command to enable voice VLAN security mode.

Use the **undo voice vlan security enable** command to disable voice VLAN security mode.

By default, voice VLAN security mode is not enabled.

Examples

Disable voice VLAN security mode.

```
<Sysname> system-view
[Sysname] undo voice vlan security enable
```

8 GVRP Configuration Commands

GVRP Configuration Commands

display garp statistics

Syntax

display garp statistics [**interface** *interface-list*]

View

Any view

Default Level

1: Monitor level

Parameters

interface *interface-list*: Defines one or multiple Ethernet ports for which the GARP statistics will be displayed. You can provide up to 10 Ethernet port lists, by each of which you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number1* **to** *interface-type interface-number2*, where the end-port number specified by *interface-number2* must be greater than the start-port number specified by *interface-number1*. If no ports are specified, this command displays the GARP statistics for all ports.

Description

Use the **display garp statistics** command to display the GARP statistics of the specified port(s) or all ports if no ports are specified.

This command displays the statistics about GVRP packets received, transmitted, and dropped on GVRP-enabled ports. When the system is restarted or after you perform the **reset garp statistics** command, the existing packet statistics are cleared and the system starts to collect new GARP statistics. With the statistics, you can judge whether a GVRP-enabled port is operating normally.

- If the number of received and transmitted GVRP packets on the port is the same as that on the remote port, it indicates that the two ends are transmitting and receiving GVRP packets normally and no registration information is lost.
- If there are dropped GVRP packets on the port, check its registration mode. GVRP packets are likely to be dropped if the registration mode is fixed or forbidden, because dynamic VLANs cannot be registered in either of the modes.

Related commands: **reset garp statistics**.

Examples

Display GARP statistics on ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
<Sysname> display garp statistics interface gigabitethernet 1/0/1 to gigabitethernet 1/0/2
```

```
GARP statistics on port GigabitEthernet1/0/1

Number of GVRP Frames Received        : 0
Number of GVRP Frames Transmitted     : 0
Number of Frames Discarded           : 0

GARP statistics on port GigabitEthernet1/0/2

Number of GVRP Frames Received        : 0
Number of GVRP Frames Transmitted     : 0
Number of Frames Discarded           : 0
```

display garp timer

Syntax

display garp timer [**interface** *interface-list*]

View

Any view

Default Level

1: Monitor level

Parameters

interface *interface-list*: Defines one or multiple Ethernet ports. You can provide up to 10 Ethernet port lists, by each of which you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number1* **to** *interface-type interface-number2*, where the end-port number specified by *interface-number2* must be greater than the start-port number specified by *interface-number1*. If no ports are specified, this command displays the GARP timer settings on all ports.

Description

Use the **display garp timer** command to display GARP timer settings of specific ports.

Related commands: **garp timer hold**, **garp timer join**, **garp timer leave**, **garp timer leaveall**.

Examples

Display GARP timers on port GigabitEthernet 1/0/1.

```
<Sysname> display garp timer interface gigabitethernet 1/0/1
      GARP timers on port GigabitEthernet1/0/1

            Garp Join Time         : 20 centiseconds
            Garp Leave Time        : 60 centiseconds
            Garp LeaveAll Time     : 1000 centiseconds
            Garp Hold Time         : 10 centiseconds
```

display gvrp local-vlan interface

Syntax

display gvrp local-vlan interface *interface-type interface-number*

View

Any view

Default Level

0: Visit level

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

Description

Use the **display gvrp local-vlan interface** command to display the local VLAN information maintained by GVRP on the specified port.

Examples

Display the local VLAN information maintained by GVRP on GigabitEthernet 1/0/1.

```
<Sysname> display gvrp local-vlan interface gigabitethernet 1/0/1
 Following VLANs exist in GVRP local database:
  1(default),2-500
```

display gvrp state

Syntax

display gvrp state interface *interface-type interface-number* **vlan** *vlan-id*

View

Any view

Default Level

0: Visit level

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

vlan *vlan-id*: Specifies a VLAN ID, in the range of 1 to 4094.

Description

Use the **display gvrp state** command to display the current GVRP state.

Examples

Display the GVRP state of VLAN 2, which GigabitEthernet 1/0/1 belongs to.

```
<Sysname> display gvrp state interface gigabitethernet 1/0/1 vlan 2
```

```
GVRP state of VLAN 2 on port GigabitEthernet1/0/1

        Applicant state machine     : VP
        Registrar state machine     : MTR
```

display gvrp statistics

Syntax

display gvrp statistics [**interface** *interface-list*]

View

Any view

Default Level

1: Monitor level

Parameters

interface *interface-list*: Defines one or multiple Ethernet ports. You can provide up to 10 Ethernet port lists, by each of which you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number1* **to** *interface-type interface-number2*, where the end-port number specified by *interface-number2* must be greater than the start-port number specified by *interface-number1*. If no ports are specified, this command displays the GVRP statistics for all trunk ports.

Description

Use the **display gvrp statistics** command to display the GVRP statistics of specified or all trunk ports.

Examples

Display statistics about GVRP for trunk port GigabitEthernet 1/0/1.

```
<Sysname> display gvrp statistics interface gigabitethernet 1/0/1
      GVRP statistics on port GigabitEthernet1/0/1

            GVRP Status                 : Enabled
            GVRP Running                : YES
            GVRP Failed Registrations     : 0
            GVRP Last Pdu Origin          : 000F-E207-F2E0
            GVRP Registration Type        : Normal
```

Table 8-1 display gvrp statistics command output description

Field	Description
GVRP Status	Indicates whether GVRP is enabled or disabled.
GVRP Running	Indicates whether GVRP is running.
GVRP Failed Registrations	Indicates the number of GVRP registration failures.
GVRP Last Pdu Origin	Indicates the source MAC address in the last GVRP PDU.
GVRP Registration Type	Indicates the GVRP registration type on the port.

display gvrp status

Syntax

display gvrp status

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display gvrp status** command to display the global enable/disable state of GVRP.

Examples

Display the global GVRP enable/disable state.

```
<Sysname> display gvrp status
            GVRP is enabled
```

display gvrp vlan-operation interface

Syntax

display gvrp vlan-operation interface *interface-type interface-number*

View

Any view

Default Level

0: Visit level

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

Description

Use the **display gvrp vlan-operation interface** command to display the information about dynamic VLAN operations performed on a port.

Examples

Display the information about dynamic VLAN operations performed on GigabitEthernet 1/0/1.

```
<Sysname> display gvrp vlan-operation interface gigabitethernet 1/0/1
       Dynamic VLAN operations on port GigabitEthernet1/0/1

              Operations of creating VLAN           : 2-100
              Operations of deleting VLAN           : none
```

```
Operations of adding VLAN to TRUNK      : 2-100
Operations of deleting VLAN from TRUNK   : none
```

garp timer hold

Syntax

garp timer hold *timer-value*

undo garp timer hold

View

Ethernet interface view, Layer-2 aggregate interface view, port group view

Default Level

2: System level

Parameters

timer-value: Hold timer setting (in centiseconds), which must be a multiple of 5 in the range of 10 (inclusive) and half of the Join timer setting (inclusive). When the Join timer is set to the default, the value range for the Hold timer is 10 (inclusive) to 10 (inclusive).

Note

One second equals 100 centiseconds.

Description

Use the **garp timer hold** command to set the GARP Hold timer for an Ethernet port, Layer-2 aggregate interface, or all ports in a port group.

Use the **undo garp timer hold** command to restore the default of the GARP Hold timer. This may fail if the default is beyond the valid value range for the Hold timer.

By default, the hold timer is set to 10 centiseconds.

Related commands: **display garp timer**, **garp timer join**.

Examples

Set the GARP Hold timer to 15 centiseconds, assuming that the Join timer is 30 centiseconds.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] garp timer hold 15
```

garp timer join

Syntax

garp timer join *timer-value*

undo garp timer join

View

Ethernet interface view, Layer-2 aggregate interface view, port group view

Default Level

2: System level

Parameters

timer-value: Join timer setting (in centiseconds), which must be a multiple of 5 in the range of two times the Hold timer (inclusive) and half of the Leave timer (inclusive). When the Hold timer and the Leave timer are set to their default, the value range for the Join timer is 20 (inclusive) to 25 (inclusive).

Description

Use the **garp timer join** command to set the GARP Join timer for an Ethernet port, Layer-2 aggregate interface, or all ports in a port group.

Use the **undo garp timer join** command to restore the default of the GARP Join timer. This may fail if the default is beyond the valid value range for the Join timer.

By default, the Join timer is set to 20 centiseconds.

Related commands: **display garp timer**, **garp timer hold**, **garp timer leave**.

Examples

Set the GARP Join timer to 25 centiseconds, assuming that both the Hold timer and the Leave timer are using the default.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] garp timer join 25
```

garp timer leave

Syntax

garp timer leave *timer-value*

undo garp timer leave

View

Ethernet interface view, Layer-2 aggregate interface view, port group view

Default Level

2: System level

Parameters

timer-value: Leave timer setting (in centiseconds), which must be a multiple of 5 between two times the Join timer (exclusive) and the LeaveAll timer setting (exclusive). When the Join timer and the LeaveAll timer are set to their default, the value range for the Leave timer is 45 (inclusive) to 995 (inclusive).

Description

Use the **garp timer leave** command to set the GARP Leave timer for an Ethernet port, Layer-2

aggregate interface, or all ports in a port group.

Use the **undo garp timer leave** command to restore the default of the GARP Leave timer. This may fail if the default is beyond the valid value range for the Leave timer.

By default, the Leave timer is set to 60 centiseconds.

Related commands: **display garp timer**, **garp timer join**, **garp timer leaveall**.

Examples

Set the GARP Leave timer to 100 centiseconds, assuming that both the Join timer and the LeaveAll timer are using the default.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] garp timer leave 100
```

garp timer leaveall

Syntax

garp timer leaveall *timer-value*

undo garp timer leaveall

View

System view

Default Level

2: System level

Parameters

timer-value: Leaveall timer setting (in centiseconds), which must be a multiple of 5 in the range of the maximum Leave timer on the device (exclusive) and 32765 (inclusive). When the Leave timers on all ports are set to the default, the value range for the LeaveAll timer is 65 (inclusive) to 32765 (inclusive).

Description

Use the **garp timer leaveall** command to set the GARP LeaveAll timer.

Use the **undo garp timer leaveall** command to restore the default. This may fail if the default is beyond the valid value range for the LeaveAll timer. .

By default, the setting of the LeaveAll timer is 1000 centiseconds.

Related commands: **display garp timer**, **garp timer leave**.

Examples

Set the leaveall timer to 100 centiseconds, assuming that the Leave timer on every port is set to 60 centiseconds.

```
<Sysname> system-view
[Sysname] garp timer leaveall 100
```

gvrp

Syntax

gvrp

undo gvrp

View

System view, Ethernet interface view, Layer-2 aggregate interface view, port group view

Default Level

2: System level

Parameters

None

Description

Use the **gvrp** command to enable GVRP globally (in system view), on a port (in Ethernet or Layer-2 aggregate interface view), or on all ports in a port group (in port group view).

Use the **undo gvrp** command to disable GVRP globally, on a port, or on all ports in a port group depending on the view where the command is executed.

By default, GVRP is disabled.

Note that:

- To enable GVRP on a port, you need to enable it globally first and then on the port.
- You can use this command on trunk ports only.
- You cannot change the link type of a GVRP-enabled trunk port.

Related commands: **display gvrp status**.

Examples

Enable GVRP globally.

```
<Sysname> system-view
[Sysname] gvrp
GVRP is enabled globally.
```

gvrp registration

Syntax

gvrp registration { **fixed** | **forbidden** | **normal** }

undo gvrp registration

View

Ethernet interface view, Layer-2 aggregate interface view, port group view

Default Level

2: System level

Parameters

fixed: Sets the registration type to fixed.

forbidden: Sets the registration type to forbidden.

normal: Sets the registration type to normal.

Description

Use the **gvrp registration** command to configure the GVRP registration type on a port (in Ethernet or Layer-2 aggregate interface view) or all ports in a port group (in port group view).

Use the **undo gvrp registration** command to restore the default on a port, or on all ports in a port group depending on the view the command is executed.

The default GVRP registration type is normal.

Note that, this command is only available on trunk ports.

Related commands: **display garp statistics**.

Examples

Set the GVRP registration type to **fixed** on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] gvrp registration fixed
```

reset garp statistics

Syntax

reset garp statistics [**interface** *interface-list*]

View

User view

Default Level

2: System level

Parameters

interface *interface-list*: Defines one or multiple Ethernet ports for which the GARP statistics are to be cleared. You can provide up to 10 Ethernet port lists, by each of which you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type interface-number1* **to** *interface-type interface-number2*, where the end-port number specified by *interface-number2* must be greater than the start-port number specified by *interface-number1*. If no ports are specified, this command clears the GARP statistics on all ports.

Description

Use the **reset garp statistics** command to clear the GARP statistics on specified ports or all ports if no ports are specified.

The cleared statistics include the statistics about GVRP packets sent, received and dropped. You can use this command in conjunction with the **display garp statistics** command to display GARP statistics.

Related commands: **display gvrp statistics**.

Examples

Clear the GARP statistics on all ports.

```
<Sysname> reset garp statistics
```

9 QinQ Configuration Commands

Note

- Throughout this document, customer network VLANs (CVLANs), also called inner VLANs, refer to the VLANs that a customer uses on the private network; and service provider network VLANs (SVLANs), also called outer VLANs, refer to the VLANs that a service provider uses to carry VLAN tagged traffic for customers.
- The selective QinQ feature of the Switch 4210G series can be achieved through the cooperation between QoS policies. For the configuration commands of traffic classes, traffic behaviors, and other QoS policy-related functions, see *QoS Commands* in the *QoS Volume*.

QinQ Configuration Commands

nest

Syntax

nest top-most vlan-id *vlan-id*

undo nest top-most

View

Traffic behavior view

Default Level

2: System Level

Parameters

vlan-id *vlan-id*: ID of the VLAN. The *vlan-id* argument is in the range 1 to 4094.

Description

Use the **nest** command to configure an outer VLAN tag for a traffic behavior.

Use the **undo nest** command to remove the outer VLAN tag.

Note that:

- The action of creating an outer VLAN tag cannot be configured simultaneously with any other action except the traffic filtering action or the action of setting 802.1p precedence in the same traffic behavior. And the action of creating an outer VLAN tag must be applied to basic QinQ-enabled ports or port groups. Otherwise, the corresponding QoS policy cannot be applied successfully.

- The **nest** action cannot be applied to a VLAN or globally.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples

Configure an outer VLAN tag for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] nest top-most vlan-id 100
```

raw-vlan-id inbound

Syntax

raw-vlan-id inbound { **all** | *vlan-list* }

undo raw-vlan-id inbound { **all** | *vlan-list* }

View

QinQ view

Default Level

2: System level

Parameters

vlan-list: Specifies one or multiple CVLANs in the format of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>. You can provide up to 10 VLAN ID lists, by each of which you can specify an individual VLAN ID in the form of *vlan-id*, or a VLAN ID range in the form of *vlan-id* **to** *vlan-id*, where the VLAN ID after **to** must be greater than the VLAN ID before **to**. The *vlan-id* argument ranges from 1 to 4094.

all: Specifies all VLAN IDs.

Description

Use the **raw-vlan-id inbound** command to tag frames of the specified CVLANs with the current SVLAN.

Use the **undo raw-vlan-id inbound** command to remove the configuration.

Caution

- You can run this command in the same view many times. A new configuration does not overwrite the previous ones and the configured values are arranged in an ascending order automatically.
- An inner VLAN tag corresponds to only one outer VLAN tag.
- If you want to change the outer VLAN tag, you need to delete the old outer tag configuration and then configure a new outer VLAN tag.

Related commands: **qinq vid**.

Examples

Configure GigabitEthernet 1/0/1 to tag frames of VLAN 3, VLAN 5, and VLAN 20 through VLAN 100 with SVLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq vid 100
[Sysname-GigabitEthernet1/0/1-vid-100] raw-vlan-id inbound 3 5 20 to 100
```

qinq enable

Syntax

qinq enable

undo qinq enable

View

Ethernet interface view, Layer-2 aggregate interface view, port group view

Default Level

2: System level

Parameters

None

Description

Use the **qinq enable** command to enable basic QinQ on the current Ethernet port(s).

Use the **undo qinq enable** command to disable basic QinQ on the current Ethernet port(s).

By default, basic QinQ is disabled on Ethernet ports.

A basic QinQ-enabled port tags received frames with the port's default VLAN tag.

Note that:

- Configuration made in Ethernet interface view takes effect on the current port only. Configuration made in Layer-2 aggregate interface view takes effect on the Layer-2 aggregate interface and the member ports in its aggregation group. Configuration made in port group view takes effect on all ports in the port group.
- You can configure this command on a Layer-2 aggregate interface and its member ports separately. Configuration made on an aggregation member port takes effect immediately. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

Examples

Enable basic QinQ on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq enable
```

Enable basic QinQ on port group 1.

```
<Sysname> system-view
```

```
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet 1/0/1 to gigabitethernet 1/0/6
[Sysname-port-group-manual-1] qinq enable
```

qinq ethernet-type

Syntax

qinq ethernet-type *hex-value*

undo qinq ethernet-type

View

System view

Default Level

2: System level

Parameters

hex-value: Hexadecimal protocol type value, in the range of 0x0001 to 0xFFFF. However, do not set it to any of the protocol type values listed in Table 9-1.

Table 9-1 Common protocol type values

Protocol type	Value
ARP	0x0806
PUP	0x0200
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1x	0x888E
Cluster	0x88A7
Reserved	0xFFFD/0xFFFE/0xFFFF

Description

Use the **qinq ethernet-type** command to configure the TPID value in VLAN tags.

Use the **undo qinq ethernet-type** command to restore the TPID value in VLAN tags to the system default

By default, the TPID value is 0x8100.

Note that :

Configuration made in system view takes effect on all ports.

Examples

Set the TPID value to 0x8200 globally.

```
<Sysname> system-view
[Sysname] qinq ethernet-type 8200
```

qinq vid

Syntax

qinq vid *vlan-id*

undo qinq vid *vlan-id*

View

Ethernet interface view, Layer-2 aggregate interface view, port group view

Default Level

2: System level

Parameters

vlan-id: Outer VLAN ID, in the range of 1 to 4094.

Description

Use the **qinq vid** command to enter QinQ view and configure the outer VLAN tag for the port to add.

Use the **undo qinq vid** command to remove all configurations corresponding to the outer VLAN ID performed in QinQ view.

By default, the outer VLAN tag is the port's default VLAN tag.

Note that:

- Configuration made in Ethernet interface view takes effect on the current port only. Configuration made in Layer-2 aggregate interface view takes effect on the Layer-2 aggregate interface and the member ports in its aggregation group. Configuration made in port group view takes effect on all ports in the port group.
- You can configure this command on a Layer-2 aggregate interface and its member ports separately. Configuration made on an aggregation member port takes effect immediately. For detailed information about link aggregation, refer to *Link Aggregation Configuration* in the *Access Volume*.

Related commands: **raw-vlan-id inbound**.

Examples

Configure GigabitEthernet 1/0/1 to tag frames with outer VLAN 10.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qinq vid 10
```

Configure all the ports in port group 1 to tag frames with outer VLAN 10.

```
<Sysname> system-view
```

```
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet 1/0/1 to gigabitethernet 1/0/6
[Sysname-port-group-manual-1] qinq vid 10
```

10 BPDU Tunneling Configuration Commands

BPDU Tunneling Configuration Commands

bpdu-tunnel dot1q

Syntax

In Ethernet interface view or port group view:

bpdu-tunnel dot1q { **cdp** | **dldp** | **eoam** | **gvrp** | **hgmp** | **lacp** | **lldp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** }

undo bpdu-tunnel dot1q { **cdp** | **dldp** | **eoam** | **gvrp** | **hgmp** | **lacp** | **lldp** | **pagp** | **pvst** | **stp** | **udld** | **vtp** }

In Layer 2 aggregate interface view:

bpdu-tunnel dot1q { **cdp** | **gvrp** | **hgmp** | **pvst** | **stp** | **vtp** }

undo bpdu-tunnel dot1q { **cdp** | **gvrp** | **hgmp** | **pvst** | **stp** | **vtp** }

View

Ethernet interface view, Layer 2 aggregate interface view, port group view

Default Level

2: System level

Parameters

cdp: Specifies to enable BPDU tunneling for the Cisco Discovery Protocol (CDP)

dldp: Specifies to enable BPDU tunneling for the Device Link Detection Protocol (DLDP)

eoam: Specifies to enable BPDU tunneling for Ethernet Operation, Administration and Maintenance (EOAM)

gvrp: Specifies to enable BPDU tunneling for the GARP VLAN Registration Protocol (GVRP)

hgmp: Specifies to enable BPDU tunneling for the HW Group Management Protocol (HGMP)

lacp: Specifies to enable BPDU tunneling for the Link Aggregation Control Protocol (LACP)

lldp: Specifies to enable BPDU tunneling for the Link Layer Discovery Protocol (LLDP)

pagp: Specifies to enable BPDU tunneling for the Port Aggregation Protocol (PAGP)

pvst: Specifies to enable BPDU tunneling for Per VLAN Spanning Tree (PVST)

stp: Specifies to enable BPDU tunneling for the Spanning Tree Protocol (STP)

udld: Specifies to enable BPDU tunneling for Uni-directional Link Direction (UDLD)

vtp: Specifies to enable BPDU tunneling for the VLAN Trunking Protocol (VTP)

Description

Use the **bpdu-tunnel dot1q** command to enable BPDU tunneling for a protocol on the current port or ports.

Use the **undo bpdu-tunnel dot1q** command to disable BPDU tunneling for a protocol on the port or ports.

By default, BPDU tunneling for any protocol is disabled.

Note that:

- Settings made in Ethernet interface view or Layer 2 aggregate interface view take effect only on the current port; settings made in port group view take effect on all ports in the port group.
- You cannot enable BPDU tunneling on a member port of a service loopback group.
- Before enabling BPDU tunneling for DLDP, EOAM, GVRP, HGMP, LLDP, or STP on a port, disable the protocol on the port first. Because PVST is a special STP protocol, before enabling BPDU tunneling for PVST on a port, you need to disable STP and then enable BPDU tunneling for STP on the port first.
- Before enabling BPDU tunneling for LACP on a dynamic aggregation group member port, remove the port from the dynamic aggregation group first.

Examples

Disable STP on GigabitEthernet1/0/1, and then enable BPDU tunneling for STP on the port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] bpdu-tunnel dot1q stp
```

Disable STP for port group 1, and then enable BPDU tunneling for STP on all the ports in the port group.

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet 1/0/1 to gigabitethernet 1/0/6
[Sysname-port-group-manual-1] undo stp enable
[Sysname-port-group-manual-1] bpdu-tunnel dot1q stp
```

Disable STP on Layer 2 aggregate interface 1, and then enable BPDU tunneling for STP on the port.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo stp enable
[Sysname-Bridge-Aggregation1] bpdu-tunnel dot1q stp
```

bpdu-tunnel tunnel-dmac

Syntax

bpdu-tunnel tunnel-dmac *mac-address*

undo bpdu-tunnel tunnel-dmac

View

System view

Default Level

2: System level

Parameters

mac-address: Destination multicast MAC address for BPDUs, in the format of H-H-H. The allowed values are 0x0100-0CCD-CDD0, 0x0100-0CCD-CDD1, 0x0100-0CCD-CDD2, and 0x010F-E200-0003.

Description

Use the **bpdu-tunnel tunnel-dmac** command to configure the destination multicast MAC address for BPDUs.

Use the **undo bpdu-tunnel tunnel-dmac** command to restore the default value.

By default, the destination multicast MAC address for BPDUs is 0x010F-E200-0003.

Examples

Set the destination multicast MAC address for BPDUs to 0x0100-0CCD-CDD0.

```
<Sysname> system-view
[Sysname] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

11 Port Mirroring Configuration Commands

Port Mirroring Configuration Commands

display mirroring-group

Syntax

display mirroring-group { *groupid* | **all** | **local** | **remote-destination** | **remote-source** }

View

Any view

Default Level

2: System level

Parameters

groupid: Number of the port mirroring group to be displayed, in the range of 1 to 4.

all: Displays all port mirroring groups.

local: Displays local mirroring groups.

remote-destination: Displays remote destination mirroring groups.

remote-source: Displays remote source port mirroring groups.

Description

Use the **display mirroring-group** command to display information about the specified port mirroring group or groups.

The output varies by port mirroring group type and is sorted by mirroring group number.

Examples

Display information about all the port mirroring groups.

```
<Sysname> display mirroring-group all
mirroring-group 1:
   type: local
   status: active
   mirroring port:
      GigabitEthernet1/0/1  both
   monitor port: GigabitEthernet1/0/10
mirroring-group 2:
   type: remote-source
   status: active
   mirroring port:
      GigabitEthernet1/0/3  both
```

```
monitor egress port: GigabitEthernet1/0/11
remote-probe vlan: 200
```

Table 11-1 Description on the fields of the **display mirroring-group** command

Field	Description
mirroring-group	Number of the port mirroring group
type	Type of the port mirroring group, which can be one of the following: local, remote-source, or remote-destination.
status	Status of the port mirroring group, which can be active or inactive.
mirroring port	Source mirroring port
monitor port	Destination mirroring port
monitor egress port	Outbound mirroring port
remote-probe vlan	Remote mirroring VLAN

mirroring-group

Syntax

mirroring-group *groupid* { **local** | **remote-destination** | **remote-source** }

undo mirroring-group { *groupid* | **all** | **local** | **remote-destination** | **remote-source** }

View

System view

Default Level

2: System level

Parameters

groupid: Specifies the number of the port mirroring group to be created or removed, in the range of 1 to 4.

all: Removes all port mirroring groups.

local: Creates a local mirroring group or removes all local mirroring groups with the **undo** command.

remote-destination: Creates a remote destination mirroring group or removes all remote destination mirroring groups with the **undo** command.

remote-source: Creates a remote source mirroring group or removes all remote source mirroring groups with the **undo** command.

Description

Use the **mirroring-group** command to create a port mirroring group.

Use the **undo mirroring-group** command to remove the specified port mirroring group or groups.

To mirror packets from a port to another port on the same device, create a local mirroring group.

To mirror packets from a port (a mirroring port) on the current device to another port (the monitor port) either on the same device or on a different device, create remote mirroring groups. When doing that,

create the remote source mirroring group on the device where the mirroring port is located and create the remote destination mirroring group on the device where the monitor port is located.

Examples

Create a local port mirroring group numbered 1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
```

Create remote destination mirroring group numbered 2.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-destination
```

mirroring-group mirroring-port

Syntax

mirroring-group *groupid* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

undo mirroring-group *groupid* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

View

System view

Default Level

2: System level

Parameters

groupid: Number of a local or remote source mirroring group, in the range of 1 to 4.

mirroring-port-list: A list of ports/port ranges to be assigned to or removed from the port mirroring group specified by *groupid*. The total number of single ports plus port ranges cannot exceed eight. In the list, a single port takes the form of *interface-type interface-number*. A port range takes the form *interface-type start-interface-number* **to** *interface-type end-interface-number*, where the end port number must be greater than the start port number.

both: Mirrors both inbound and outbound packets on the specified port(s).

inbound: Mirrors only inbound packets on the specified port(s).

outbound: Mirrors only outbound packets on the specified port(s).

Description

Use the **mirroring-group mirroring-port** command to assign ports to a local or remote source mirroring group as mirroring ports.

Use the **undo mirroring-group mirroring-port** command to remove mirroring ports from the mirroring group.

By configuring a port as a mirroring port, you can track the packets received from or/and sent out the port.

Before you can assign a port to a mirroring group, create the mirroring group first.

Note that:

- A mirroring port cannot be a member port of an existing port mirroring group.

- You cannot add a mirroring port for a remote destination mirroring group.
- When removing a mirroring port from a mirroring group, make sure the traffic direction you specified in the **undo mirroring-group mirroring-port** command matches the actual monitored direction of the port.

Examples

Configure mirroring ports in port mirroring group 1, assuming that the mirroring group already exists.

```
<Sysname> system-view
[Sysname] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/5
both
```

Remove source mirroring ports from port mirroring group 1.

```
[Sysname] undo mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 to GigabitEthernet
1/0/3 both
```

mirroring-group monitor-egress

Syntax

In system view:

mirroring-group *groupid* **monitor-egress** *monitor-egress-port-id*

undo mirroring-group *groupid* **monitor-egress** *monitor-egress-port-id*

In Ethernet port view:

mirroring-group *groupid* **monitor-egress**

undo mirroring-group *groupid* **monitor-egress**

View

System view, Ethernet port view

Default Level

2: System level

Parameters

groupid: Number of a remote source mirroring group, in the range of 1 to 4.

monitor-egress-port-id: Port to be configured as the egress port. It takes the form of *interface-type interface-number*, where *interface-type* specifies the port type and *interface-number* specifies the port number.

Description

Use the **mirroring-group monitor-egress** command to configure a port as the egress port in a remote source mirroring group.

Use the **undo mirroring-group monitor-egress** command to remove the egress port from the mirroring group.

Note that:

- Only remote source port mirroring groups can have outbound mirroring ports. A port mirroring group can have only one outbound mirroring port.

- The outbound port cannot be a member port of the current mirroring group.
- It is not recommended to configure STP, RSTP, MSTP, 802.1X, IGMP Snooping, static ARP and MAC address learning on the outbound mirroring port; otherwise, the mirroring function may be affected.

Examples

Configure port GigabitEthernet 1/0/1 as the egress port of remote source mirroring group 1 in system view.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 monitor-egress GigabitEthernet 1/0/1
```

Configure port GigabitEthernet 1/0/2 as the egress port of remote source mirroring group 2 in Ethernet port view.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] mirroring-group 2 monitor-egress
```

mirroring-group monitor-port

Syntax

mirroring-group *groupid* **monitor-port** *monitor-port-id*

undo mirroring-group *groupid* **monitor-port** *monitor-port-id*

View

System view

Default Level

2: System level

Parameters

groupid: Number of a local or remote destination mirroring group, in the rang of 1 to 4.

monitor-port-id: Port to be assigned to the specified mirroring group as the monitor port. The argument takes the form of *interface-type interface-number*, where *interface-type* specifies the port type and *interface-number* specifies the port number.

Description

Use the **mirroring-group monitor-port** command to assign a port to a local or remote destination mirroring group as the monitor port.

Use the **undo mirroring-group monitor-port** command to remove the monitor port from the local or remote destination mirroring group.

Note that:

- Before assigning a port to a mirroring group, make sure that the group already exists.
- A port mirroring group can contain only one destination port.
- The destination port cannot be a member port of the current mirroring group.

- The destination mirroring port can be an access, trunk, or hybrid port. It must be assigned to the remote mirroring VLAN.
- A remote source port mirroring group cannot contain destination ports.
- Before configuring the destination port for a port mirroring group, make sure the port mirroring group exists.
- Do not enable STP, RSTP, or MSTP on the destination port. Otherwise, the mirroring function may be affected.
- Do not use the destination mirroring port for any purpose other than port mirroring.

Examples

Configure GigabitEthernet 1/0/1 as the monitor port in remote destination mirroring group 1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-destination
[Sysname] mirroring-group 1 monitor-port GigabitEthernet 1/0/1
```

mirroring-group remote-probe vlan

Syntax

mirroring-group *groupid* **remote-probe vlan** *rprobe-vlan-id*

undo mirroring-group *groupid* **remote-probe vlan** *rprobe-vlan-id*

View

System view

Default Level

2: System level

Parameters

groupid: Number of a remote source or destination mirroring group, in the range of 1 to 4.

rprobe-vlan-id: ID of the VLAN to be configured as the remote probe VLAN. This VLAN must be a static VLAN that already exists.

Description

Use the **mirroring-group remote-probe vlan** command to specify a VLAN as the remote probe VLAN for a remote source or destination mirroring group.

Use the **undo mirroring-group remote-probe vlan** command to remove the remote probe VLAN from the remote source or destination mirroring group.

Note that:

- Only remote source port mirroring groups or remote destination port mirroring groups can have remote mirroring VLANs. A port mirroring group can have only one remote mirroring VLAN.
- To remove a VLAN operating as a remote port mirroring VLAN, you need to restore it to a normal VLAN first. A remote port mirroring group gets invalid if the corresponding remote port mirroring VLAN is removed.
- You are recommended to use a remote mirroring VLAN for remote mirroring only.

Examples

Specify VLAN 2 as the remote probe VLAN of port mirroring group 1, assuming that VLAN 2 already exists.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
[Sysname] mirroring-group 1 remote-probe vlan 2
```

mirroring-port

Syntax

[**mirroring-group** *groupid*] **mirroring-port** { **inbound** | **outbound** | **both** }

undo [**mirroring-group** *groupid*] **mirroring-port** { **inbound** | **outbound** | **both** }

View

Ethernet port view

Default Level

2: System level

Parameters

groupid: Number of a local or remote source mirroring group, in the range of 1 to 4.

both: Mirrors both inbound and outbound packets on the current port.

inbound: Mirrors only inbound packets on the current port.

outbound: Mirrors only outbound packets on the current port.

Description

Use the **mirroring-port** command to assign the current port to a local or remote source mirroring group as a mirroring port.

Use the **undo mirroring-port** command to remove the current port from the port mirroring group.

When assigning a port to a mirroring group as a mirroring port, note that:

- If no mirroring group is specified, the port is assigned to port mirroring group 1.
- Whether you assign the port to port mirroring group 1 or any other mirroring group, ensure that the mirroring group already exists.
- A mirroring port cannot be a member port of an existing port mirroring group.
- You cannot add a mirroring port for a remote destination mirroring group.
- When removing a mirroring port from a mirroring group, make sure the traffic direction you specified in the **undo** [**mirroring-group** *groupid*] **mirroring-port** command matches the actual monitored direction of the port.

Examples

Configure GigabitEthernet 1/0/1 as a source mirroring port of remote source port mirroring group 2.

```
<Sysname> system-view
[Sysname] mirroring-group 2 remote-source
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mirroring-group 2 mirroring-port both
```

monitor-port

Syntax

[**mirroring-group** *groupid*] **monitor-port**

undo [**mirroring-group** *groupid*] **monitor-port**

View

Ethernet port view

Default Level

2: System level

Parameters

groupid: Number of a local or remote destination mirroring group, in the range of 1 to 4.

Description

Use the **monitor-port** command to assign the current port to a local or remote destination mirroring group as the monitor port.

Use the **undo monitor-port** command to remove the current port from the mirroring group.

When assigning a port to a mirroring group as the monitor port, note that:

- If no mirroring group is specified, the port is assigned to port mirroring group 1.
- The port cannot belong to any other mirroring group.
- Whether you assign the port to port mirroring group 1 or any other mirroring group, ensure that the mirroring group already exists.
- The remote destination mirroring port can be an access, trunk, or hybrid port. It must be assigned to the remote mirroring VLAN.
- Do not enable STP, RSTP, or MSTP on the destination port. Otherwise, the mirroring function may be affected.
- Do not use the destination mirroring port for any purpose other than port mirroring.

Examples

Configure GigabitEthernet 1/0/1 as the monitor port in local mirroring group numbered 1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] monitor-port
```

Table of Contents

1 IP Addressing Configuration Commands

IP Addressing Configuration Commands

display ip interface

Syntax

display ip interface [*interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Description

Use the **display ip interface** command to display information about a specified or all Layer 3 interfaces.

Examples

Display information about interface VLAN-interface 1.

```
<Sysname> display ip interface vlan-interface 1
Vlan-interface1 current state : DOWN
Line protocol current state : DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
ARP packet input number:         0
  Request packet:               0
  Reply packet:                 0
  Unknown packet:               0
TTL invalid packet number:        0
ICMP packet input number:         0
  Echo reply:                   0
  Unreachable:                  0
  Source quench:                0
  Routing redirect:             0
  Echo request:                 0
```

```
Router advert:                0
Router solicit:               0
Time exceed:                  0
IP header bad:                0
Timestamp request:            0
Timestamp reply:              0
Information request:          0
Information reply:            0
Netmask request:              0
Netmask reply:                0
Unknown type:                 0
```

Table 1-1 display ip interface command output description

Field	Description
current state	Current physical state of the interface, which can be • Administrative DOWN: Indicates that the interface is administratively down; that is, the interface is shut down with the **shutdown** command. • DOWN: Indicates that the interface is administratively up but its physical state is down, which may be caused by a connection or link failure. • UP: Indicates that both the administrative and physical states of the interface are up.
Line protocol current state	Current state of the link layer protocol, which can be • DOWN: Indicates that the protocol state of the interface is down, which is usually because that no IP address is assigned to the interface. • UP: Indicates that the protocol state of the interface is up.
Internet Address	IP address of an interface followed by: • Primary: Identifies a primary IP address, or • Sub: Identifies a secondary IP address.
Broadcast address	Broadcast address of the subnet attached to an interface
The Maximum Transmit Unit	Maximum transmission units on the interface, in bytes
input packets, bytes, multicasts output packets, bytes, multicasts	Unicast packets, bytes, and multicast packets received on an interface (the statistics start at the device startup)
ARP packet input number: Request packet: Reply packet: Unknown packet:	Total number of ARP packets received on the interface (the statistics start at the device startup), including • ARP request packets • ARP reply packets • Unknown packets
TTL invalid packet number	Number of TTL-invalid packets received on the interface (the statistics start at the device startup)

Field	Description
ICMP packet input number: Echo reply: Unreachable: Source quench: Routing redirect: Echo request: Router advert: Router solicit: Time exceed: IP header bad: Timestamp request: Timestamp reply: Information request: Information reply: Netmask request: Netmask reply: Unknown type:	Total number of ICMP packets received on the interface (the statistics start at the device startup), including the following packets: • Echo reply packet • Unreachable packets • Source quench packets • Routing redirect packets • Echo request packets • Router advertisement packets • Router solicitation packets • Time exceeded packets • IP header bad packets • Timestamp request packets • Timestamp reply packets • Information request packets • Information reply packets • Netmask request packets • Netmask reply packets • Unknown type packets

display ip interface brief

Syntax

display ip interface brief [*interface-type* [*interface-number*]]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type: Interface type.

interface-number: Interface number.

Description

Use the **display ip interface brief** command to display brief information about a specified or all layer 3 interfaces.

Without the interface type and interface number specified, the information about all layer 3 interfaces is displayed; with only the interface type specified, the information about all layer 3 interfaces of the specified type is displayed; with both the interface type and interface number specified, only the information about the specified interface is displayed.

Related commands: **display ip interface**.

Examples

Display brief information about VLAN interfaces.

```
<Sysname> display ip interface brief vlan-interface
*down: administratively down
(s): spoofing
Interface                Physical Protocol IP Address     Description
Vlan-interface1           up       up       6.6.6.6        Vlan-inte...
Vlan-interface2           up       up       7.7.7.7        Vlan-inte...
```

Table 1-2 display ip interface brief command output description

Field	Description
*down: administratively down	The interface is administratively shut down with the **shutdown** command.
(s) : spoofing	Spoofing attribute of the interface. It indicates that an interface whose network layer protocol is displayed up may have no link present or the link is set up only on demand.
Interface	Interface name
Physical	Physical state of the interface, which can be • *down: Indicates that the interface is administratively down; that is, the interface is shut down with the **shutdown** command. • down: Indicates that the interface is administratively up but its physical state is down, which may be caused by a connection or link failure. • up: Indicates that both the administrative and physical states of the interface are up.
Protocol	Link layer protocol state of the interface, which can be • down: Indicates that the protocol state of the interface is down, which is usually because that no IP address is assigned to the interface. • up: Indicates that the protocol state of the interface is up.
IP Address	IP address of the interface (If no IP address is configured, “unassigned” is displayed.)
Description	Interface description information, for which at most 12 characters can be displayed. If there are more that 12 characters, only the first nine characters are displayed.

ip address

Syntax

ip address *ip-address* { *mask* | *mask-length* } [**sub**]

undo ip address [*ip-address* { *mask* | *mask-length* } [**sub**]]

View

Interface view

Default Level

2: System level

Parameters

ip-address: IP address of interface, in dotted decimal notation.

mask: Subnet mask in dotted decimal notation.

mask-length: Subnet mask length, the number of consecutive ones in the mask.

sub: Secondary IP address for the interface.

Description

Use the **ip address** command to assign an IP address and mask to the interface.

Use the **undo ip address** command to remove all IP addresses from the interface.

Use the **undo ip address** *ip-address* { *mask* | *mask-length* } command to remove the primary IP address.

Use the **undo ip address** *ip-address { mask* | *mask-length* } **sub** command to remove a secondary IP address.

By default, no IP address is assigned to any interface.

When assigning IP addresses to an interface, consider the following:

- You can assign only one primary IP address to an interface.
- The primary and secondary IP addresses can be located in the same network segment.
- Before removing the primary IP address, remove all secondary IP addresses.
- You cannot assign a secondary IP address to the interface that is configured to borrow an IP address through IP unnumbered or obtain one through BOOTP, or DHCP.

Related commands: **display ip interface**.

Examples

Assign VLAN-interface 1 a primary IP address 129.12.0.1 and a secondary IP address 202.38.160.1, with subnet masks being 255.255.255.0.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 129.12.0.1 255.255.255.0
[Sysname-Vlan-interface1] ip address 202.38.160.1 255.255.255.0 sub
```

2 ARP Configuration Commands

ARP Configuration Commands

arp check enable

Syntax

arp check enable

undo arp check enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **arp check enable** command to enable ARP entry check. With this function enabled, the device cannot learn any ARP entry with a multicast MAC address. Configuring such a static ARP entry is not allowed either; otherwise, the system displays error messages.

Use the **undo arp check enable** command to disable the function. After the ARP entry check is disabled, the device can learn the ARP entry with a multicast MAC address, and you can also configure such a static ARP entry on the device.

By default, ARP entry check is enabled.

Examples

Enable ARP entry check.

```
<Sysname> system-view
[Sysname] arp check enable
```

arp max-learning-num

Syntax

arp max-learning-num *number*

undo arp max-learning-num

View

Ethernet interface view, VLAN interface view, Layer-2 aggregate interface view

Default Level

2: System level

Parameters

number: Maximum number of dynamic ARP entries that a interface can learn. The value is in the range 0 to 256.

Description

Use the **arp max-learning-num** command to configure the maximum number of dynamic ARP entries that a interface can learn.

Use the **undo arp max-learning-num** command to restore the default.

By default, the maximum number of dynamic ARP entries that a interface can learn is 256.

Examples

Specify VLAN-interface 40 to learn up to 200 dynamic ARP entries.

```
<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40] arp max-learning-num 200
```

arp static

Syntax

arp static *ip-address mac-address* [*vlan-id interface-type interface-number*]

undo arp ip-address

View

System view

Default Level

2: System level

Parameters

ip-address: IP address in an ARP entry.

mac-address: MAC address in an ARP entry, in the format H-H-H.

vlan-id: ID of a VLAN to which a static ARP entry belongs to, in the range 1 to 4094.

interface-type interface-number: Interface type and interface number.

Description

Use the **arp static** command to configure a static ARP entry in the ARP mapping table.

Use the **undo arp** command to remove an ARP entry.

Note that:

- A static ARP entry is effective when the device works normally. However, when the VLAN or VLAN interface to which an ARP entry corresponds is deleted, the entry, if permanent, will be deleted, and if non-permanent and resolved, will become unresolved.

- The vlan-id argument is used to specify the corresponding VLAN of an ARP entry and must be the ID of an existing VLAN. In addition, the Ethernet interface following the argument must belong to that VLAN. The VLAN interface of the VLAN must have been created.

Related commands: **reset arp**, **display arp**.

Examples

Configure a static ARP entry, with the IP address being 202.38.10.2, the MAC address being 000f-e201-0000, and the outbound interface being GigabitEthernet 1/0/1 of VLAN 10.

```
<Sysname> system-view
[Sysname] arp static 202.38.10.2 000f-e201-0000 10 gigabitethernet 1/0/1
```

arp timer aging

Syntax

arp timer aging *aging-time*

undo arp timer aging

View

System view

Default Level

2: System level

Parameters

aging-time: Aging time for dynamic ARP entries in minutes, in the range 1 to 1,440.

Description

Use the **arp timer aging** command to set aging time for dynamic ARP entries.

Use the **undo arp timer aging** command to restore the default.

By default, the aging time for dynamic ARP entries is 20 minutes.

Related commands: **display arp timer aging**.

Examples

Set aging time for dynamic ARP entries to 10 minutes.

```
<Sysname> system-view
[Sysname] arp timer aging 10
```

display arp

Syntax

display arp [[**all** | **dynamic** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [[**|** { **begin** | **exclude** | **include** } *regular-expression*] | **count**]

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays all ARP entries.

dynamic: Displays dynamic ARP entries.

static: Displays static ARP entries.

slot *slot-number*: Displays the ARP entries for the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

vlan *vlan-id*: Displays the ARP entries of the specified VLAN. The VLAN ID ranges from 1 to 4,094.

interface *interface-type interface-number:* Displays the ARP entries of the interface specified by the argument *interface-type interface-number*.

|: Uses a regular expression to specify the ARP entries to be displayed. For detailed information about regular expressions, refer to *Basic System Configuration* in the *System Volume*.

begin: Displays ARP entries from the first one containing the specified string.

exclude: Displays the ARP entries that do not contain the specified string.

include: Displays the ARP entries containing the specified string.

regular-expression: A case-sensitive string for matching, consisting of 1 to 256 characters.

count: Displays the number of ARP entries.

Description

Use the **display arp** command to display ARP entries in the ARP mapping table.

If no parameter is specified, all ARP entries are displayed.

Related commands: **arp static**, **reset arp**.

Examples

Display the detailed information of all ARP entries.

```
<Sysname> display arp all
              Type: S-Static    D-Dynamic
IP Address      MAC Address     VLAN ID  Interface           Aging Type
192.168.0.18    000f-3d80-2b38  1        GE1/0/22            18    D
192.168.0.57    00e0-fc00-000b  1        GE1/0/22            20    D
192.168.0.56    000f-cb00-5601  1        GE1/0/22            20    D
192.168.0.6     0015-e943-712f  1        GE1/0/22            16    D
```

Table 2-1 display arp command output description

Field	Description
IP Address	IP address in an ARP entry
MAC Address	MAC address in an ARP entry
VLAN ID	VLAN ID contained a static ARP entry
Interface	Outbound interface in an ARP entry

Field	Description
Aging	Aging time for a dynamic ARP entry in minutes (“N/A” means unknown aging time or no aging time)
Type	ARP entry type: D for dynamic, S for static
Vpn-instance Name	Name of VPN instance. [No Vrf] means no VPN instance is configured for the corresponding ARP.

Display the number of all ARP entries.

```
<Sysname> display arp all count
 Total entry(ies):  4
```

display arp *ip-address*

Syntax

display arp *ip-address* [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

ip-address: Displays the ARP entry for the specified IP address.

slot *slot-number*: Displays the ARP entry for the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

|: Uses a regular expression to specify the ARP entries to be displayed. For detailed information about regular expressions, refer to *Basic System Configuration* in the *System Volume*.

begin: Displays the ARP entries from the first one containing the specified string.

exclude: Displays the ARP entries that do not contain the specified string.

include: Displays the ARP entries that contain the specified string.

regular-expression: A case-sensitive string for matching, consisting of 1 to 256 characters.

Description

Use the **display arp** *ip-address* command to display the ARP entry for a specified IP address.

Related commands: **arp static**, **reset arp**.

Examples

Display the corresponding ARP entry for the IP address 20.1.1.1.

```
<Sysname> display arp 20.1.1.1
             Type: S-Static    D-Dynamic
IP Address      MAC Address     VLAN ID  Interface           Aging Type
20.1.1.1        00e0-fc00-0001  N/A      N/A                 N/A   S
```

display arp timer aging

Syntax

display arp timer aging

View

Any view

Default Level

2: System level

Parameters

None

Description

Use the **display arp timer aging** command to display the aging time for dynamic ARP entries.

Related commands: **arp timer aging**.

Examples

Display the aging time for dynamic ARP entries.

```
<Sysname> display arp timer aging
Current ARP aging time is 10 minute(s)
```

reset arp

Syntax

reset arp { **all** | **dynamic** | **slot** *slot-number* | **static** | **interface** *interface-type interface-number* }

View

User view

Default Level

2: System level

Parameters

all: Clears all ARP entries except authorized ARP entries.

dynamic: Clears all dynamic ARP entries.

static: Clears all static ARP entries.

slot *slot-number*: Clears the ARP entries for the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

interface *interface-type interface-number*: Clears the ARP entries for the interface specified by the argument *interface-type interface-number*.

Description

Use the **reset arp** command to clear ARP entries except authorized ARP entries from the ARP mapping table.

With **interface** *interface-type interface-number* or **slot** *slot-number* specified, the command clears only dynamic ARP entries of the interface or the specified device in the IRF.

Related commands: **arp static**, **display arp**.

Examples

Clear all static ARP entries.

```
<Sysname> reset arp static
```

Gratuitous ARP Configuration Commands

gratuitous-arp-sending enable

Syntax

gratuitous-arp-sending enable

undo gratuitous-arp-sending enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **gratuitous-arp-sending enable** command to enable a device to send gratuitous ARP packets when receiving ARP requests from another network segment.

Use the **undo gratuitous-arp-sending enable** command to restore the default.

By default, a device cannot send gratuitous ARP packets when receiving ARP requests from another network segment.

Examples

Disable a device from sending gratuitous ARP packets.

```
<Sysname> system-view
[Sysname] undo gratuitous-arp-sending enable
```

gratuitous-arp-learning enable

Syntax

gratuitous-arp-learning enable

undo gratuitous-arp-learning enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **gratuitous-arp-learning enable** command to enable the gratuitous ARP packet learning function.

Use the **undo gratuitous-arp-learning enable** command to disable the function.

By default, the function is enabled.

With this function enabled, a device receiving a gratuitous ARP packet can add the source IP and MAC addresses carried in the packet to its own dynamic ARP table if it finds no ARP entry in the cache corresponding to the source IP address of the ARP packet exists; if the corresponding ARP entry exists in the cache, the device updates the ARP entry regardless of whether this function is enabled.

Examples

Enable the gratuitous ARP packet learning function.

```
<Sysname> system-view
[Sysname] gratuitous-arp-learning enable
```

3 Proxy ARP Configuration Commands

Proxy ARP Configuration Commands

display local-proxy-arp

Syntax

display local-proxy-arp [**interface vlan-interface** *vlan-id*]

View

Any view

Default Level

2: System level

Parameters

interface vlan-interface *vlan-id*: Displays the local proxy ARP status of the specified VLAN interface.

Description

Use the **display local-proxy-arp** command to display the status of the local proxy ARP.

Related commands: **local-proxy-arp enable**.

Examples

Display the status of the local proxy ARP on VLAN-interface 2.

```
<Sysname> display local-proxy-arp interface vlan-interface 2
Interface Vlan-interface2
 Local Proxy ARP status: enabled
```

display proxy-arp

Syntax

display proxy-arp [**interface vlan-interface** *vlan-id*]

View

Any view

Default Level

2: System level

Parameters

interface vlan-interface *vlan-id*: Displays the proxy ARP status of the VLAN interface specified by the argument *vlan-id*.

Description

Use the **display proxy-arp** command to display the proxy ARP status.

If an interface is specified, proxy ARP status of the specified interface is displayed; if no interface is specified, proxy ARP status of all interfaces is displayed.

Related commands: **proxy-arp enable**.

Examples

Display the proxy ARP status on VLAN-interface 1.

```
<Sysname> display proxy-arp interface vlan-interface 1
 Proxy ARP status: disabled
```

local-proxy-arp enable

Syntax

local-proxy-arp enable

undo local-proxy-arp enable

View

VLAN interface view

Default Level

2: System level

Parameters

None

Description

Use the **local-proxy-arp enable** command to enable local proxy ARP.

Use the **undo local-proxy-arp enable** command to disable local proxy ARP.

By default, local proxy ARP is disabled.

Related commands: **display local-proxy-arp**.

Examples

Enable local proxy ARP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable
```

proxy-arp enable

Syntax

proxy-arp enable

undo proxy-arp enable

View

VLAN interface view

Default Level

2: System level

Parameters

None

Description

Use the **proxy-arp enable** command to enable proxy ARP.

Use the **undo proxy-arp enable** command to disable proxy ARP.

By default, proxy ARP is disabled.

Related commands: **display proxy-arp**.

Examples

Enable proxy ARP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] proxy-arp enable
```

4 ARP Attack Defense Configuration Commands

ARP Source Suppression Configuration Commands

arp source-suppression enable

Syntax

arp source-suppression enable

undo arp source-suppression enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **arp source-suppression enable** command to enable the ARP source suppression function.

Use the **undo arp source-suppression enable** command to disable the function.

By default, the ARP source suppression function is disabled.

Related commands: **display arp source-suppression**.

Examples

Enable the ARP source suppression function.

```
<Sysname> system-view
[Sysname] arp source-suppression enable
```

arp source-suppression limit

Syntax

arp source-suppression limit *limit-value*

undo arp source-suppression limit

View

System view

Default Level

2: System level

Parameters

limit-value: Specifies the maximum number of packets with the same source IP address but unresolvable destination IP addresses that the device can receive in five seconds. It ranges from 2 to 1024.

Description

Use the **arp source-suppression limit** command to set the maximum number of packets with the same source IP address but unresolvable destination IP addresses that the device can receive in five seconds.

Use the **undo arp source-suppression limit** command to restore the default value, which is 10.

With this feature configured, whenever the number of packets with unresolvable destination IP addresses from a host within five seconds exceeds the specified threshold, the device suppress the sending host from triggering any ARP requests within the following five seconds.

Related commands: **display arp source-suppression**.

Examples

Set the maximum number of packets with the same source address but unresolvable destination IP addresses that the device can receive in five seconds to 100.

```
<Sysname> system-view
[Sysname] arp source-suppression limit 100
```

display arp source-suppression

Syntax

display arp source-suppression

View

Any view

Default Level

2: System level

Parameters

None

Description

Use the **display arp source-suppression** command to display information about the current ARP source suppression configuration.

Examples

Display information about the current ARP source suppression configuration.

```
<Sysname> display arp source-suppression
 ARP source suppression is enabled
 Current suppression limit: 100
 Current cache length: 16
```

Table 4-1 display arp source-suppression command output description

Field	Description
ARP source suppression is enabled	The ARP source suppression function is enabled
Current suppression limit	Maximum number of packets with the same source IP address but unresolvable IP addresses that the device can receive in five seconds
Current cache length	Size of cache used to record source suppression information

ARP Defense Against IP Packet Attack Configuration Commands

arp resolving-route enable

Syntax

arp resolving-route enable

undo arp resolving-route enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **arp resolving-route enable** command to enable ARP defense against IP packet attacks.

Use the **undo arp resolving-route enable** command to disable the function.

By default, the function of ARP defense against IP packet attacks is enabled.

Examples

Disable ARP defense against IP packet attacks.

```
<Sysname> system-view
[Sysname] undo arp resolving-route enable
```

ARP Active Acknowledgement Configuration Commands

arp anti-attack active-ack enable

Syntax

arp anti-attack active-ack enable

undo arp anti-attack active-ack enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **arp anti-attack active-ack enable** command to enable the ARP active acknowledgement function.

Use the **undo arp anti-attack active-ack enable** command to restore the default.

By default, the ARP active acknowledgement function is disabled.

Typically, this feature is configured on gateway devices to identify invalid ARP packets.

With this feature enabled, the gateway, upon receiving an ARP packet with a different source MAC address from that in the corresponding ARP entry, checks whether the ARP entry has been updated within the last minute:

- If yes, the ARP entry is not updated;
- If not, the gateway sends a unicast request to the source MAC address of the ARP entry.

Then,

- If a response is received within five seconds, the ARP packet is ignored;
- If no response is received, the gateway sends a unicast request to the source MAC address of the ARP packet.

Then,

- If a response is received within five seconds, the gateway updates the ARP entry;
- If not, the ARP entry is not updated.

Examples

Enable the ARP active acknowledgement function.

```
<Sysname> system-view
[Sysname] arp anti-attack active-ack enable
```

Source MAC Address Based ARP Attack Detection Configuration Commands

arp anti-attack source-mac

Syntax

arp anti-attack source-mac { **filter** | **monitor** }

undo arp anti-attack source-mac [**filter** | **monitor**]

View

System view

Default Level

2: System level

Parameters

filter: Specifies the **filter** mode.

monitor: Specifies the **monitor** mode.

Description

Use the **arp anti-attack source-mac** command to enable source MAC address based ARP attack detection and specify the detection mode.

Use the **undo arp anti-attack source-mac** command to restore the default.

By default, source MAC address based ARP attack detection is disabled.

After you enable this feature, the device checks the source MAC address of ARP packets received from the VLAN. If the number of ARP packets received from a source MAC address within five seconds exceeds the specified threshold:

- In filter detection mode, the device displays an alarm and filters out the ARP packets from the MAC address.
- In monitor detection mode, the device only displays an alarm.

Note that: If no detection mode is specified in the **undo arp anti-attack source-mac** command, both detection modes are disabled.

Examples

Enable filter-mode source MAC address based ARP attack detection

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac filter
```

arp anti-attack source-mac aging-time

Syntax

arp anti-attack source-mac aging-time *time*

undo arp anti-attack source-mac aging-time

View

System view

Default Level

2: System level

Parameters

time: Aging timer for protected MAC addresses, in the range of 60 to 6000 seconds.

Description

Use the **arp anti-attack source-mac aging-time** command to configure the aging timer for protected MAC addresses.

Use the **undo arp anti-attack source-mac aging-time** command to restore the default.

By default, the aging timer for protected MAC addresses is 300 seconds (five minutes).

Examples

Configure the aging timer for protected MAC addresses as 60 seconds.

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac aging-time 60
```

arp anti-attack source-mac exclude-mac

Syntax

arp anti-attack source-mac exclude-mac *mac-address*&<1-n>

undo arp anti-attack source-mac exclude-mac [*mac-address*&<1-n>]

View

System view

Default Level

2: System level

Parameters

mac-address&<1-n>: MAC address list. The *mac-address* argument indicates a protected MAC address in the format H-H-H. &<1-n> indicates the number of protected MAC addresses that you can configure. The maximum of the n argument is 10.

Description

Use the **arp anti-attack source-mac exclude-mac** command to configure protected MAC addresses which will be excluded from ARP packet detection.

Use the **undo arp anti-attack source-mac exclude-mac** command to remove the configured protected MAC addresses.

By default, no protected MAC address is configured.

Note that: If no MAC address is specified in the **undo arp anti-attack source-mac exclude-mac** command, all the configured protected MAC addresses are removed.

Examples

Configure a protected MAC address.

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac exclude-mac 2-2-2
```

arp anti-attack source-mac threshold

Syntax

arp anti-attack source-mac threshold *threshold-value*

undo arp anti-attack source-mac threshold

View

System view

Default Level

2: System level

Parameters

threshold-value: Threshold for source MAC address based ARP attack detection, in the range 10 to 100.

Description

Use the **arp anti-attack source-mac threshold** command to configure the threshold for source MAC address based ARP attack detection. If the number of ARP packets sent from a MAC address within five seconds exceeds this threshold, the device considers this an attack.

Use the **undo arp anti-attack source-mac threshold** command to restore the default.

By default, the threshold for source MAC address based ARP attack detection is 50.

Examples

Configure the threshold for source MAC address based ARP attack detection as 30.

```
<Sysname> system-view
[Sysname] arp anti-attack source-mac threshold 30
```

display arp anti-attack source-mac

Syntax

display arp anti-attack source-mac { **slot** *slot-number* | **interface** *interface-type interface-number* }

View

Any view

Default Level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays attacking MAC addresses detected on the interface.

slot *slot-number*: Displays attacking MAC addresses detected on the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

Description

Use the **display arp anti-attack source-mac** command to display attacking MAC addresses detected by source MAC address based ARP attack detection.

On a device, if no interface is specified, the **display arp anti-attack source-mac** command displays attacking MAC addresses detected on all the interfaces.

Examples

Display the attacking MAC addresses detected by source MAC address based ARP attack detection.

```
<Sysname> display arp anti-attack source-mac slot 1
Source-MAC        VLAN-ID         Interface           Aging-time
23f3-1122-3344     4094           GE1/0/1             10
23f3-1122-3355     4094           GE1/0/2             30
23f3-1122-33ff     4094           GE1/0/3             25
23f3-1122-33ad     4094           GE1/0/4             30
23f3-1122-33ce     4094           GE1/0/5             2
```

ARP Packet Source MAC Address Consistency Check Configuration Commands

arp anti-attack valid-ack enable

Syntax

arp anti-attack valid-check enable

undo arp anti-attack valid-check enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **arp anti-attack valid-check enable** command to enable ARP packet source MAC address consistency check on the gateway. After you execute this command, the gateway device can filter out ARP packets with the source MAC address in the Ethernet header different from the sender MAC address in the ARP message.

Use the **undo arp anti-attack valid-check enable** command to disable ARP packet source MAC address consistency check.

By default, ARP packet source MAC address consistency check is disabled.

Examples

Enable ARP packet source MAC address consistency check.

```
<Sysname> system-view
[Sysname] arp anti-attack valid-check enable
```

ARP Packet Rate Limit Configuration Commands

arp rate-limit

Syntax

arp rate-limit { **disable** | **rate** *pps* **drop** }

undo arp rate-limit

View

Layer 2 Ethernet port view

Default Level

2: System level

Parameters

disable: Disables ARP packet rate limit.

rate *pps*: ARP packet rate in pps, in the range 50 to 500.

drop: Discards the exceeded packets.

Description

Use the **arp rate-limit** command to configure or disable ARP packet rate limit. If a rate is specified, exceeded packets are discarded.

Use the **undo arp rate-limit** command to restore the default.

By default, ARP packet rate limit is enabled, and the ARP packet rate limit is 100 pps.

Examples

Specify the ARP packet rate on GigabitEthernet 1/0/1 as 60 pps, and exceeded packets are discarded.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp rate-limit rate 60 drop
```

ARP Detection Configuration Commands

arp detection enable

Syntax

arp detection enable

undo arp detection enable

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **arp detection enable** command to enable ARP detection for the VLAN.

Use the **undo arp detection enable** command to disable ARP detection for the VLAN.

By default, ARP detection is disabled for a VLAN.

Examples

Enable ARP detection for VLAN 1.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-Vlan1] arp detection enable
```

arp detection mode

Syntax

arp detection mode { **dhcp-snooping** | **dot1x | static-bind** }

undo arp detection mode { **dhcp-snooping** | **dot1x | static-bind** }

View

System view

Default Level

2: System level

Parameters

dhcp-snooping: Implements ARP attack detection based on DHCP snooping entries. This mode is mainly used to prevent source address spoofing attacks.

dot1x: Implements ARP attack detection based on 802.1X security entries. This mode is mainly used to prevent source address spoofing attacks.

static-bind: Implements ARP attack detection based on static IP-to-MAC binding entries. This mode is mainly used to prevent gateway spoofing attacks.

Description

Use the **arp detection mode** command to specify an ARP attack detection mode.

Use the **undo arp detection mode** command to cancel the specified ARP detection mode.

By default, no ARP detection mode is specified, that is, all packets are considered to be invalid.

Note that, if you specify the three modes at the same time, the system uses static IP-to-MAC bindings first, then DHCP snooping entries, and then 802.1X security entries.

Examples

Enable ARP detection based on both DHCP snooping entries and 802.1X security entires.

```
<Sysname> system-view
[Sysname] arp detection mode dhcp-snooping
[Sysname] arp detection mode dot1x
```

arp detection static-bind

Syntax

arp detection static-bind *ip-address mac-address*

undo arp detection static-bind [*ip-address*]

View

System view

Default Level

2: System level

Parameters

ip-address: IP address of the static binding.

mac-address: MAC address of the static binding, in the format of H-H-H.

Description

Use the **arp detection static-bind** command to configure a static IP-to-MAC binding.

Use the **undo arp detection static-bind** command to remove the configure static binding.

By default, no static IP-to-MAC binding is configured.

With ARP detection based on static IP-to-MAC bindings configured, the device, upon receiving an ARP packet from an ARP trusted/untrusted port, compares the source IP and MAC addresses of the ARP packet against the static IP-to-MAC bindings.

- If an entry with a matching IP address but different MAC address is found, the ARP packet is considered invalid and discarded.
- If an entry with both matching IP and MAC addresses is found, the ARP packet is considered valid and can pass the detection.
- If no match is found, the ARP packet is considered valid and can pass the detection.

Note that: If no IP address is specified in the **undo arp detection static-bind** command, all configured static IP-to-MAC bindings are removed.

Examples

Configure a static IP-to-MAC binding.

```
<Sysname> system-view
[Sysname] arp detection static-bind 192.168.1.2 2-1-201
```

arp detection trust

Syntax

arp detection trust

undo arp detection trust

View

Layer 2 Ethernet port view

Default Level

2: System level

Parameters

None

Description

Use the **arp detection trust** command to configure the port as an ARP trusted port.

Use the **undo arp detection trust** command to configure the port as an ARP untrusted port.

By default, the port is an ARP untrusted port.

Examples

Configure GigabitEthernet 1/0/1 as an ARP trusted port.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp detection trust
```

arp detection validate

Syntax

arp detection validate { **dst-mac** | **ip | src-mac** } *

undo arp detection validate [**dst-mac** | **ip** | **src-mac**] *

View

System view

Default Level

2: System level

Parameters

dst-mac: Checks the target MAC address of ARP responses. If the target MAC address is all-zero, all-one, or inconsistent with the destination MAC address in the Ethernet header, the packet is considered invalid and discarded.

ip: Checks the source and destination IP addresses of ARP packets. The all-zero, all-one or multicast IP addresses are considered invalid and the corresponding packets are discarded. With this keyword specified, the source and destination IP addresses of ARP replies, and the source IP address of ARP requests will be checked.

src-mac: Checks whether the source MAC address of an ARP packet is identical to that in its Ethernet header. If they are identical, the packet is considered valid; otherwise, the packet is discarded.

Description

Use the **arp detection validate** command to configure ARP detection based on specified objects. You can specify one or more objects in one command line.

Use the **undo arp detection validate** command to remove detected objects. If no keyword is specified, all the detected objects are removed.

By default, ARP detection based on specified objects is disabled.

Examples

Enable the checking of the MAC addresses and IP addresses of ARP packets.

```
<Sysname> system-view
[Sysname] arp detection validate dst-mac src-mac ip
```

display arp detection

Syntax

display arp detection

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display arp detection** command to display the VLAN(s) enabled with ARP detection.

Related commands: **arp detection enable**.

Examples

Display the VLANs enabled with ARP detection.

```
<Sysname> display arp detection
ARP detection is enabled in the following VLANs:
1, 2, 4-5
```

Table 4-2 display arp detection command output description

Field	Description
ARP detection is enabled in the following VLANs	VLANs that are enabled with ARP detection

display arp detection statistics

Syntax

display arp detection statistics [**interface** *interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the ARP detection statistics of a specified interface.

Description

Use the **display arp detection statistics** command to display statistics about ARP detection. This command only displays numbers of discarded packets. If no interface is specified, the statistics of all the interfaces will be displayed.

Examples

Display the ARP detection statistics of all the interfaces.

```
<Sysname> display arp detection statistics
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)        IP        Src-MAC    Dst-MAC    Inspect
GE1/0/1(U)              40        0          0          78
GE1/0/2(U)              0         0          0          0
GE1/0/3(T)              0         0          0          0
GE1/0/4(U)              0         0          30         0
```

Table 4-3 display arp detection statistics command output description

Field	Description
Interface(State)	State T or U identifies a trusted or untrusted port.
IP	Number of ARP packets discarded due to invalid source and destination IP addresses
Src-MAC	Number of ARP packets discarded due to invalid source MAC address
Dst-MAC	Number of ARP packets discarded due to invalid destination MAC address
Inspect	Number of ARP packets that failed to pass ARP detection (based on DHCP snooping entries/802.1X security entries/static IP-to-MAC bindings)

reset arp detection statistics

Syntax

reset arp detection statistics [**interface** *interface-type interface-number*]

View

User view

Default Level

2: System level

Parameters

interface *interface-type interface-number*: Clears the ARP detection statistics of a specified interface.

Description

Use the **reset arp detection statistics** command to clear ARP detection statistics of a specified interface. If no interface is specified, the statistics of all the interfaces will be cleared.

Examples

Clear the ARP detection statistics of all the interfaces.

```
<Sysname> reset arp detection statistics
```

5 DHCP Relay Agent Configuration Commands

Note

The DHCP relay agent configuration is supported only on VLAN interfaces.

DHCP Relay Agent Configuration Commands

dhcp relay address-check

Syntax

dhcp relay address-check { **disable** | **enable** }

View

Interface view

Default Level

2: System level

Parameters

disable: Disables IP address match check on the relay agent.

enable: Enables IP address match check on the relay agent.

Description

Use the **dhcp relay address-check enable** command to enable IP address match check on the relay agent.

Use the **dhcp relay address-check disable** command to disable IP address match check on the relay agent.

By default, the function is disabled.

If a requesting client's IP and MAC addresses do not match any binding (both dynamic and static bindings) on the DHCP relay agent, the client cannot access external networks via the DHCP relay agent.

Note that: The **dhcp relay address-check enable** command only checks IP and MAC addresses of clients.

Examples

Enable IP address match check on the DHCP relay agent.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay address-check enable
```

dhcp relay information circuit-id format-type

Syntax

dhcp relay information circuit-id format-type { **ascii** | **hex** }

undo dhcp relay information circuit-id format-type

View

Interface view

Default Level

2: System level

Parameters

ascii: Specifies the code type for the circuit ID sub-option as **ascii**.

hex: Specifies the code type for the circuit ID sub-option as **hex**.

Description

Use the **dhcp relay information circuit-id format-type** command to configure the code type for the non-user-defined circuit ID sub-option.

Use the **undo dhcp relay information circuit-id format-type** command to restore the default.

By default, the code type for the circuit ID sub-option depends on the specified padding format of Option 82. Each field has its own code type.

Note that:

This command applies to configuring the non-user-defined circuit ID sub-option only. After you configure the padding content for the circuit ID sub-option using the **dhcp relay information circuit-id string** command, ASCII is adopted as the code type.

Examples

Configure the code type for the non-user-defined circuit ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information circuit-id format-type ascii
```

dhcp relay information circuit-id string

Syntax

dhcp relay information circuit-id string *circuit-id*

undo dhcp relay information circuit-id string

View

Interface view

Default Level

2: System level

Parameters

circuit-id: Padding content for the user-defined circuit ID sub-option, a case-sensitive string of 3 to 63 characters.

Description

Use the **dhcp relay information circuit-id string** command to configure the padding content for the user-defined circuit ID sub-option.

Use the **undo dhcp relay information circuit-id string** command to restore the default.

By default, the padding content for the circuit ID sub-option depends on the padding format of Option 82.

Note that:

After you configure the padding content for the circuit ID sub-option using this command, ASCII is adopted as the code type.

Related commands: **dhcp relay information format**.

Examples

Configure the padding content for the circuit ID sub-option as **company001**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information circuit-id string company001
```

dhcp relay information enable

Syntax

dhcp relay information enable

undo dhcp relay information enable

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **dhcp relay information enable** command to enable the relay agent to support Option 82.

Use the **undo dhcp relay information enable** command to disable Option 82 support.

By default, Option 82 support is disabled on DHCP relay agent.

Examples

Enable Option 82 support on the relay agent.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
```

dhcp relay information format

Syntax

dhcp relay information format { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] }

undo dhcp relay information format [**verbose node-identifier**]

View

Interface view

Default Level

2: System level

Parameters

normal: Specifies the normal padding format.

verbose: Specifies the verbose padding format.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies access node identifier. By default, the node MAC address is used as the node identifier.

- **mac** indicates using MAC address as the node identifier.
- **sysname** indicates using the device name of a node as the node identifier.
- **user-defined** *node-identifier* indicates using a specified character string as the node identifier, in which *node-identifier* is a string with 1 to 50 characters.

Description

Use the **dhcp relay information format** command to specify a padding format for Option 82.

Use the **undo dhcp relay information format** command to restore the default padding format.

The Option 82 padding format defaults to **normal**.

Note

- Using the **undo dhcp relay information format** command without the keyword **verbose node-identifier** restores the default **normal** padding format, or with the keyword **verbose node-identifier** restores the **mac** mode of the **verbose** padding format.
- If configuring the handling strategy of the DHCP relay agent as **replace**, you need to configure a padding format of Option 82. If the handling strategy is **keep** or **drop**, you need not configure any padding format.
- If sub-option 1 (node identifier) of Option 82 is padded with the device name (sysname) of a node, the device name must contain no spaces. Otherwise, the DHCP relay agent will drop the message.

Examples

Specify the verbose padding format for Option 82.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
[Sysname-Vlan-interface1] dhcp relay information strategy replace
[Sysname-Vlan-interface1] dhcp relay information format verbose
```

dhcp relay information remote-id format-type

Syntax

dhcp relay information remote-id format-type { **ascii** | **hex** }

undo dhcp relay information remote-id format-type

View

Interface view

Default Level

2: System view

Parameters

ascii: Specifies the code type for the remote ID sub-option as **ascii**.

hex: Specifies the code type for the remote ID sub-option as **hex**.

Description

Use the **dhcp relay information remote-id format-type** command to configure the code type for the non-user-defined remote ID sub-option.

Use the **undo dhcp relay information remote-id format-type** command to restore the default.

By default, the code type for the remote ID sub-option is HEX.

Note that:

This command applies to configuring the non-user-defined remote ID sub-option only. After you configure the padding content for the remote ID sub-option using the **dhcp relay information remote-id string** command, ASCII is adopted as the code type.

Examples

Configure the code type for the non-user-defined remote ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information remote-id format-type ascii
```

dhcp relay information remote-id string

Syntax

dhcp relay information remote-id string { *remote-id* | **sysname** }

undo dhcp relay information remote-id string

View

Interface view

Default Level

2: System level

Parameters

remote-id: Padding content for the user-defined remote ID sub-option, a case sensitive string of 1 to 63 characters.

sysname: Specifies the device name as the padding content for the remote ID sub-option.

Description

Use the **dhcp relay information remote-id string** command to configure the padding content for the user-defined remote ID sub-option.

Use the **undo dhcp relay information remote-id string** command to restore the default.

By default, the padding content for the remote ID sub-option depends on the padding format of Option 82.

Note that: After you configure the padding content for the remote ID sub-option using this command, ASCII is adopted as the code type.

Related commands: **dhcp relay information format**.

Note

If you want to specify the character string **sysname** (a case-insensitive character string) as the padding content for the remote ID sub-option, you need to use quotation marks to make it take effect. For example, if you want to specify **Sysname** as the padding content for the remote ID sub-option, you need to enter the **dhcp relay information remote-id string** “Sysname” command.

Examples

Configure the padding content for the remote ID sub-option as **device001**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information remote-id string device001
```

dhcp relay information strategy

Syntax

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

View

Interface view

Default Level

2: System level

Parameters

drop: Specifies to drop messages containing Option 82.

keep: Specifies to forward messages containing Option 82 without any change.

replace: Specifies to forward messages containing Option 82 after replacing the original Option 82 with the Option 82 padded in the specified padding format.

Description

Use the **dhcp relay information strategy** command to configure DHCP relay agent handling strategy for messages containing Option 82.

Use the **undo dhcp relay information strategy** command to restore the default handling strategy.

The handling strategy for messages containing Option 82 defaults to **replace**.

Examples

Configure the DHCP relay agent handling strategy for messages containing Option 82 as **keep**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay information enable
[Sysname-Vlan-interface1] dhcp relay information strategy keep
```

dhcp relay release ip

Syntax

dhcp relay release ip *client-ip*

View

System view

Default Level

2: System level

Parameters

client-ip: DHCP client IP address.

Description

Use the **dhcp relay release ip** command to request the DHCP server to release a specified client IP address.

Examples

Request the DHCP server to release the IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp relay release ip 1.1.1.1
```

dhcp relay security static

Syntax

dhcp relay security static *ip-address mac-address* [**interface** *interface-type interface-number*]

undo dhcp relay security { *ip-address* | **all** | **dynamic** | **interface** *interface-type interface-number* | **static** }

View

System view

Default Level

2: System level

Parameters

ip-address: Client IP address for creating a static binding.

mac-address: Client MAC address for creating a static binding, in the format H-H-H.

interface *interface-type interface-number*: Specifies a Layer 3 interface connecting to the DHCP client. *interface-type interface-number* specifies the interface type and interface number.

all: Specifies all client entries to be removed.

dynamic: Specifies dynamic client entries to be removed.

static: Specifies manual client entries to be removed.

Description

Use the **dhcp relay security static** command to configure a static client entry, that is, the binding between IP address, MAC address, and Layer 3 interface on the relay agent.

Use the **undo dhcp relay security** command to remove specified client entries from the relay agent.

No manual client entry is configured on the DHCP relay agent by default.

Note that:

- When using the **dhcp relay security static** command to bind an interface to a static client entry, make sure that the interface is configured as a DHCP relay agent; otherwise, entry conflicts may occur.
- The **undo dhcp relay security interface** command is used to remove all the dynamic client entries from the interface.

Related commands: **display dhcp relay security**.

Examples

Bind DHCP relay interface VLAN-interface 2 to IP address 10.10.1.1 and MAC address 0005-5d02-f2b3 of the client.

```
<Sysname> system-view
[Sysname] dhcp relay security static 10.10.1.1 0005-5d02-f2b3 interface vlan-interface 2
```

dhcp relay security tracker

Syntax

dhcp relay security tracker { *interval* | **auto** }

undo dhcp relay security tracker [*interval*]

View

System view

Default Level

2: System level

Parameters

interval: Refreshing interval in seconds, in the range of 1 to 120.

auto: Specifies the **auto** refreshing interval, which is the value of 60 seconds divided by the number of binding entries. Thus, the more entries are, the shorter interval is, but the shortest interval is no less than 500 ms.

Description

Use the **dhcp relay security tracker** command to set a refreshing interval at which the relay agent contacts the DHCP server for refreshing dynamic bindings.

Use the **undo dhcp relay security tracker** command to restore the default interval.

The default refreshing interval is **auto**, the value of 60 seconds divided by the number of binding entries.

Examples

Set the refreshing interval as 100 seconds.

```
<Sysname> system-view
[Sysname] dhcp relay security tracker 100
```

dhcp relay server-detect

Syntax

dhcp relay server-detect

undo dhcp relay server-detect

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **dhcp relay server-detect** command to enable unauthorized DHCP server detection.

Use the **undo dhcp relay server-detect** command to disable unauthorized DHCP server detection.

By default, unauthorized DHCP server detection is disabled.

With this function enabled, upon receiving a DHCP request, the DHCP relay agent will record the IP addresses of all DHCP servers which ever offered IP addresses to the DHCP client and the receiving interface. Each server detected is recorded only once. The administrator can get this information from logs to check out unauthorized DHCP servers.

After the information of recorded DHCP servers is cleared, the relay agent will re-record server information following this mechanism.

Examples

Enable unauthorized DHCP server detection.

```
<Sysname> system-view
[Sysname] dhcp relay server-detect
```

dhcp relay server-group

Syntax

dhcp relay server-group *group-id* **ip** *ip-address*

undo dhcp relay server-group *group-id* [**ip** *ip-address*]

View

System view

Default Level

2: System level

Parameters

group-id: DHCP server group number, in the range of 0 to 19.

ip *ip-address*: DHCP server IP address.

Description

Use the **dhcp relay server-group** command to specify a DHCP server for a DHCP server group.

Use the **undo dhcp relay server-group** command to remove a DHCP server from a DHCP server group, if no **ip** *ip-address* is specified, all servers in the DHCP server group and the server group itself will be removed.

By default, no DHCP server is specified for a DHCP server group.

Note that:

- The IP address of any DHCP server and any interface's IP address of the DHCP relay agent cannot be in the same network segment. Otherwise, the client may fail to obtain an IP address.
- If a server group has been correlated to multiple interfaces, you need to cancel these correlations before removing the server group.

Related commands: **display dhcp relay server-group**.

Examples

Specify DHCP server 1.1.1.1 for DHCP server group 1 on the relay agent.

```
<Sysname> system-view
[Sysname] dhcp relay server-group 1 ip 1.1.1.1
```

dhcp relay server-select

Syntax

dhcp relay server-select *group-id*

undo dhcp relay server-select

View

Interface view

Default Level

2: System level

Parameters

group-id: DHCP server group number to be correlated, in the range of 0 to 19.

Description

Use the **dhcp relay server-select** command to correlate specified interface(s) to a specified DHCP server group.

Use the **undo dhcp relay server-select** command to remove a configured correlation.

By default, no DHCP server group is correlated with an interface on the relay agent.

Note that:

- A DHCP server group can correlate with one or multiple DHCP relay agent interfaces.
- A relay agent interface can only correlate with one DHCP server group, and a newly configured correlation overwrites the previous one. If the server group in the new correlation does not exist, the new configuration will not work. The interface still maintains the previous correlation.

- The DHCP server group referenced in this command should have been configured by using the **dhcp relay server-group** command.

Related commands: **dhcp relay server-group**.

Examples

Correlate VLAN-interface 1 to DHCP server group 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp relay server-select 1
```

dhcp select relay

Syntax

dhcp select relay

undo dhcp select relay

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **dhcp select relay** command to enable the relay agent on the current interface. Upon receiving requests from an enabled interface, the relay agent will forward these requests to outside DHCP servers for IP address allocation.

Use the **undo dhcp select relay** command to restore the default.

After DHCP is enabled, the DHCP server is enabled on an interface by default. That is, upon receiving a client's request from the interface, the DHCP server allocates an IP address from the DHCP address pool to the client.

When the working mode of the interface is changed from DHCP server to DHCP relay agent, neither the IP address leases nor the authorized ARP entries will be deleted. However, these ARP entries may conflict with new ARP entries generated on the DHCP relay agent; therefore, you are recommended to delete the existing IP address leases when changing the interface working mode to DHCP relay agent.

Examples

Enable the DHCP relay agent on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] dhcp select relay
```

display dhcp relay

Syntax

display dhcp relay { **all** | **interface** *interface-type interface-number* }

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays information of DHCP server groups that all interfaces correspond to.

interface *interface-type interface-number*: Displays information of the DHCP server group that a specified interface corresponds to.

Description

Use the **display dhcp relay** command to display information about DHCP server groups correlated to an interface or all interfaces.

Examples

Display information about DHCP server groups correlated to all interfaces.

```
<Sysname> display dhcp relay all
   Interface name          Server-group
   Vlan-interface1         2
```

Table 5-1 display dhcp relay all command output description

Field	Description
Interface name	Interface name
Server-group	DHCP server group number correlated to the interface.

display dhcp relay information

Syntax

display dhcp relay information { **all** | **interface** *interface-type interface-number* }

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays the Option 82 configuration information of all interfaces.

interface *interface-type interface-number*: Displays the Option 82 configuration information of a specified interface.

Description

Use the **display dhcp relay information** command to display Option 82 configuration information on the DHCP relay agent.

Examples

Display the Option 82 configuration information of all interfaces.

```
<Sysname> display dhcp relay information all
Interface: Vlan-interface100
    Status: Enable
    Strategy: Replace
    Format: Verbose
    Circuit ID format-type: HEX
    Remote ID format-type: ASCII
    Node identifier: abaci
    User defined:
        Circuit ID: company001
Interface: Vlan-interface200
    Status: Enable
    Strategy: Keep
    Format: Normal
    Circuit ID format-type: HEX
    Remote ID format-type: ASCII
    User defined:
        Remote ID: device001
```

display dhcp relay security

Syntax

display dhcp relay security [*ip-address* | **dynamic** | **static**]

View

Any view

Default Level

1: Monitor level

Parameters

ip-address: Displays the binding information of an IP address.

dynamic: Displays information about dynamic bindings.

static: Displays information about static bindings.

Description

Use the **display dhcp relay security** command to display information about bindings of DHCP relay agents. If no parameter is specified, information about all bindings will be displayed.

Examples

Display information about all bindings.

```
<Sysname> display dhcp relay security
IP Address      MAC Address     Type      Interface
 10.1.1.1       00e0-0000-0001  Static    Vlan1
 10.1.1.5       00e0-0000-0000  Static    Vlan2
---   2 dhcp-security item(s) found   ---
```

Table 5-2 display dhcp relay security command output description

Field	Description
IP Address	Client IP address
MAC Address	Client MAC address
Type	Type of binding, including dynamic, static, and temporary.
Interface	Layer 3 interface connecting to the DHCP client. If no interface is recorded in the binding entry, “N/A” is displayed.

display dhcp relay security statistics

Syntax

display dhcp relay security statistics

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display dhcp relay security statistics** command to display statistics information about bindings of DHCP relay agents.

Examples

Display statistics about bindings of DHCP relay agents.

```
<Sysname> display dhcp relay security statistics
Static Items     :1
Dynamic Items    :0
Temporary Items  :0
All Items        :1
```

Table 5-3 display dhcp relay security statistics command output description

Field	Description
Static Items	Static binding items
Dynamic Items	Dynamic binding items
Temporary Items	Temporary binding items
All Items	All binding items

display dhcp relay security tracker

Syntax

display dhcp relay security tracker

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display dhcp relay security tracker** command to display the interval for refreshing dynamic bindings on the relay agent.

Examples

Display the interval for refreshing dynamic bindings on the relay agent.

```
<Sysname> display dhcp relay security tracker
 Current tracker interval : 10s
```

The interval is 10 seconds.

display dhcp relay server-group

Syntax

display dhcp relay server-group { *group-id* | **all** }

View

Any view

Default Level

1: Monitor level

Parameters

group-id: Displays the information of the specified DHCP server group numbered from 0 to 19.

all: Displays the information of all DHCP server groups.

Description

Use the **display dhcp relay server-group** command to display the configuration information of a specified or all DHCP server groups.

Examples

Display IP addresses of DHCP servers in DHCP server group 1.

```
<Sysname> display dhcp relay server-group 1
   No.          Group IP
   1            1.1.1.1
   2            1.1.1.2
```

Table 5-4 display dhcp relay server-group command output description

Field	Description
No.	Sequence number
Group IP	IP address in the server group

display dhcp relay statistics

Syntax

display dhcp relay statistics [**server-group** { *group-id* | **all** }]

View

Any view

Default Level

1: Monitor level

Parameters

group-id: Specifies a server group number in the range of 0 to 19 about which to display DHCP packet statistics.

all: Specifies all server groups about which to display DHCP packet statistics. Information for each group will be displayed.

Description

Use the **display dhcp relay statistics** command to display DHCP packet statistics related to a specified or all DHCP server groups.

Note that if no parameter (**server-group** and **all)** is specified, all DHCP packet statistics on the relay agent will be displayed.

Examples

Display all DHCP packet statistics on the relay agent.

```
<Sysname> display dhcp relay statistics
```

```
    Bad packets received:                0
    DHCP packets received from clients:     0
       DHCPDISCOVER packets received:      0
       DHCPREQUEST packets received:       0
       DHCPINFORM packets received:        0
       DHCPRELEASE packets received:       0
       DHCPDECLINE packets received:       0
       BOOTPREQUEST packets received:      0
    DHCP packets received from servers:     0
       DHCPOFFER packets received:         0
       DHCPACK packets received:           0
       DHCPNAK packets received:           0
       BOOTPREPLY packets received:        0
    DHCP packets relayed to servers:        0
       DHCPDISCOVER packets relayed:       0
       DHCPREQUEST packets relayed:        0
       DHCPINFORM packets relayed:         0
       DHCPRELEASE packets relayed:        0
       DHCPDECLINE packets relayed:        0
       BOOTPREQUEST packets relayed:       0
    DHCP packets relayed to clients:        0
       DHCPOFFER packets relayed:          0
       DHCPACK packets relayed:            0
       DHCPNAK packets relayed:            0
       BOOTPREPLY packets relayed:         0
    DHCP packets sent to servers:           0
       DHCPDISCOVER packets sent:          0
       DHCPREQUEST packets sent:           0
       DHCPINFORM packets sent:            0
       DHCPRELEASE packets sent:           0
       DHCPDECLINE packets sent:           0
       BOOTPREQUEST packets sent:          0
    DHCP packets sent to clients:           0
       DHCPOFFER packets sent:             0
       DHCPACK packets sent:               0
       DHCPNAK packets sent:               0
       BOOTPREPLY packets sent:            0
```

Display DHCP packet statistics related to every server group on the relay agent.

```
<Sysname> display dhcp relay statistics server-group all
DHCP relay server-group          #0
    Packet type             Packet number
 Client -> Server:
    DHCPDISCOVER                 0
    DHCPREQUEST                  0
    DHCPINFORM                   0
    DHCPRELEASE                  0
    DHCPDECLINE                  0
```

```
    BOOTPREQUEST                0
Server -> Client:
    DHCPOFFER                   0
    DHCPACK                     0
    DHCPNAK                     0
    BOOTPREPLY                  0
```

reset dhcp relay statistics

Syntax

reset dhcp relay statistics [**server-group** *group-id*]

View

User view

Default Level

1: Monitor level

Parameters

server-group *group-id*: Specifies a server group ID (in the range of 0 to 19) about which to remove statistics from the relay agent.

Description

Use the **reset dhcp relay statistics** command to remove statistics from the relay agent.

If no **server-group** is specified, all statistics will be removed from the relay agent.

Related commands: **display dhcp relay statistics**.

Examples

Remove all statistics from the DHCP relay agent.

```
<Sysname> reset dhcp relay statistics
```

6 DHCP Client Configuration Commands

Note

- The DHCP client configuration is supported only on VLAN interfaces.
- When multiple VLAN interfaces having the same MAC address use DHCP for IP address acquisition via a relay agent, the DHCP server cannot be the Windows 2000 Server or Windows 2003 Server.
- You are not recommended to enable both the DHCP client and the DHCP snooping on the same device. Otherwise, DHCP snooping entries may fail to be generated, or the DHCP client may fail to obtain an IP address.

DHCP Client Configuration Commands

display dhcp client

Syntax

display dhcp client [**verbose**] [**interface** *interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

verbose: Specifies verbose DHCP client information to be displayed.

interface *interface-type interface-number*: Specifies an interface of which to display DHCP client information.

Description

Use the **display dhcp client** command to display DHCP client information. If no **interface** *interface-type interface-number* is specified, DHCP client information of all interfaces will be displayed.

Examples

Display DHCP client information of all interfaces.

```
<Sysname> display dhcp client
Vlan-interface1 DHCP client information:
```

```
 Current machine state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 DHCP server: 40.1.1.2
```

Display verbose DHCP client information.

```
<Sysname> display dhcp client verbose
Vlan-interface1 DHCP client information:
 Current machine state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 Lease from 2005.08.13 15:37:59   to   2005.08.16 15:37:59
 DHCP server: 40.1.1.2
 Transaction ID: 0x1c09322d
 Default router: 40.1.1.2
 Classless static route:
   Destination: 1.1.0.1, Mask: 255.0.0.0, NextHop: 192.168.40.16
   Destination: 10.198.122.63, Mask: 255.255.255.255, NextHop: 192.168.40.16
 DNS server: 44.1.1.11
 DNS server: 44.1.1.12
 Domain name: ddd.com
 Boot server: 200.200.200.200  1.1.1.1
 Client ID: 3030-3066-2e65-3234-
           392e-3830-3438-2d56-
           6c61-6e2d-696e-7465-
           7266-6163-6531
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.
```

Table 6-1 display dhcp client command output description

Field	Description
Vlan-interface1 DHCP client information	Information of the interface acting as the DHCP client
Current machine state	DHCP client current machine state
Allocated IP	The IP address allocated by the DHCP server
Allocated lease	The allocated lease time
T1	The 1/2 lease time (in seconds) of the DHCP client IP address
T2	The 7/8 lease time (in seconds) of the DHCP client IP address
Lease from….to….	The start and end time of the lease.
DHCP Server	DHCP server IP address that assigned the IP address
Transaction ID	Transaction ID, a random number chosen by the client to identify an IP address allocation.
Default router	The gateway address assigned to the client
Classless static route	Classless static routes assigned to the client
Static route	Classful static routes assigned to the client

Field	Description
DNS server	The DNS server address assigned to the client
Domain name	The domain name suffix assigned to the client
Boot server	PXE server addresses (up to 16 addresses) specified for the DHCP client, which are obtained through Option 43.
Client ID	Client ID
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	How long the T1 (1/2 lease time) timer will timeout.

ip address dhcp-alloc

Syntax

ip address dhcp-alloc [**client-identifier mac** *interface-type interface-number*]

undo ip address dhcp-alloc

View

Interface view

Default Level

2: System level

Parameters

client-identifier mac *interface-type interface-number*: Specifies the MAC address of an interface using which as the client ID to obtain an IP address.

Description

Use the **ip address dhcp-alloc** command to configure an interface to use DHCP for IP address acquisition.

Use the **undo ip address dhcp-alloc** command to cancel an interface from using DHCP.

By default, an interface does not use DHCP for IP address acquisition.

Note that:

- If no parameter is specified, the client uses a character string comprised of the current interface name and MAC address as its ID for address acquisition.
- The DHCP client sends a DHCP-RELEASE message for releasing the IP address obtained via DHCP, if the interface of the client is down, the message cannot be sent.
- For a sub interface that obtained an IP address via DHCP, using the **shutdown** command on its primary interface does not make the DHCP client send a DHCP-RELEASE message for releasing the sub interface's IP address.

Examples

Configure VLAN-interface 1 to use DHCP for IP address acquisition.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address dhcp-alloc
```

7 DHCP Snooping Configuration Commands

Note

- The DHCP snooping enabled device does not work if it is between the DHCP relay agent and DHCP server, and it can work when it is between the DHCP client and relay agent or between the DHCP client and server.
- You are not recommended to enable the DHCP client, BOOTP client, and DHCP snooping on the same device. Otherwise, DHCP snooping entries may fail to be generated, or the BOOTP client/DHCP client may fail to obtain an IP address.

DHCP Snooping Configuration Commands

dhcp-snooping

Syntax

dhcp-snooping

undo dhcp-snooping

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **dhcp-snooping** command to enable DHCP snooping.

Use the **undo dhcp-snooping** command to disable DHCP snooping.

With DHCP snooping disabled, all ports can forward responses from any DHCP servers and does not record binding information about MAC addresses of DHCP clients and the obtained IP addresses.

By default, DHCP snooping is disabled.

Related commands: **display dhcp-snooping**.

Examples

Enable DHCP snooping.

```
<Sysname> system-view
[Sysname] dhcp-snooping
```

dhcp-snooping information circuit-id format-type

Syntax

dhcp-snooping information circuit-id format-type { **ascii** | **hex** }

undo dhcp-snooping information circuit-id format-type

View

Layer 2 Ethernet port view

Default Level

2: System level

Parameters

ascii: Specifies the code type for the circuit ID sub-option as **ascii**.

hex: Specifies the code type for the circuit ID sub-option as **hex**.

Description

Use the **dhcp-snooping information circuit-id format-type** command to configure the code type for the non-user-defined circuit ID sub-option.

Use the **undo dhcp-snooping information circuit-id format-type** command to restore the default.

By default, the code type for the circuit ID sub-option depends on the padding format of Option 82. Each field has its own code type.

Note that:

This command applies to configuring the non-user-defined circuit ID sub-option only. After you configure the padding content for the circuit ID sub-option using the **dhcp-snooping information circuit-id string** command, ASCII is adopted as the code type.

Examples

Configure the padding format for the non-user-defined circuit ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabiEthernet1/0/1] dhcp-snooping information circuit-id format-type ascii
```

dhcp-snooping information circuit-id string

Syntax

dhcp-snooping information [**vlan** *vlan-id*] **circuit-id string** *circuit-id*

undo dhcp-snooping information [**vlan** *vlan-id*] **circuit-id string**

View

Layer 2 Ethernet port view

Default Level

2: System level

Parameters

vlan *vlan-id*: Specifies a VLAN ID, in the range of 1 to 4094.

circuit-id: Padding content for the user-defined circuit ID sub-option, a case-sensitive string of 3 to 63 characters.

Description

Use the **dhcp-snooping information circuit-id string** command to configure the padding content for the user-defined circuit ID sub-option.

Use the **undo dhcp-snooping information circuit-id string** command to restore the default.

By default, the padding content for the circuit ID sub-option depends on the padding format of Option 82.

Note that:

- After you configure the padding content for the circuit ID sub-option using this command, ASCII is adopted as the code type.
- If a VLAN is specified, the configured circuit ID sub-option only takes effect within the VLAN; if no VLAN is specified, the configured circuit ID sub-option takes effect in all VLANs. The former case has a higher priority; that is, the circuit ID sub-option specified for a VLAN will be padded for packets within the VLAN.

Related commands: **dhcp-snooping information format**.

Examples

Configure the global padding content for the user-defined circuit ID sub-option as **company001**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabiEthernet1/0/1] dhcp-snooping information circuit-id string company001
```

dhcp-snooping information enable

Syntax

dhcp-snooping information enable

undo dhcp-snooping information enable

View

Layer 2 Ethernet interface view

Default Level

2: System level

Parameters

None

Description

Use the **dhcp-snooping information enable** command to configure DHCP snooping to support Option 82.

Use the **undo dhcp-snooping information enable** command to disable this function.

By default, DHCP snooping does not support Option 82.

Examples

Configure DHCP snooping to support Option 82.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabiEthernet1/0/1] dhcp-snooping information enable
```

dhcp-snooping information format

Syntax

dhcp-snooping information format { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] }

undo dhcp-snooping information format [**verbose node-identifier**]

View

Layer 2 Ethernet interface view

Default Level

2: System level

Parameters

normal: Specifies the normal padding format.

verbose: Specifies the verbose padding format.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies access node identifier. By default, the node MAC address is used as the node identifier.

- **mac** indicates using MAC address as the node identifier.
- **sysname** indicates using the device name of a node as the node identifier.
- **user-defined** *node-identifier* indicates using a specified character string as the node identifier, in which *node-identifier* is a string of 1 to 50 characters.

Description

Use the **dhcp-snooping information format** command to specify the padding format for Option 82.

Use the **undo dhcp-snooping information format command** to restore the default.

By default, the padding format for Option 82 is **normal**.

Note that when you use the **undo dhcp-snooping information format** command, if the **verbose node-identifier** argument is not specified, the padding format will be restored to **normal**; if the **verbose node-identifier** argument is specified, the padding format will be restored to **verbose** with MAC address as the node identifier.

Examples

Specify the padding format as **verbose** for Option 82.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabiEthernet1/0/1] dhcp-snooping information enable
[Sysname-GigabiEthernet1/0/1] dhcp-snooping information strategy replace
[Sysname-GigabiEthernet1/0/1] dhcp-snooping information format verbose
```

dhcp-snooping information remote-id format-type

Syntax

dhcp-snooping information remote-id format-type { **ascii** | **hex** }

undo dhcp-snooping information remote-id format-type

View

Layer 2 Ethernet port view

Default Level

2: System level

Parameters

ascii: Specifies the code type for the remote ID sub-option as **ascii**.

hex: Specifies the code type for the remote ID sub-option as **hex**.

Description

Use the **dhcp-snooping information remote-id format-type** command to configure the code type for the non-user-defined remote ID sub-option.

Use the **undo dhcp-snooping information remote-id format-type** command to restore the default.

By default, the code type for the remote ID sub-option is HEX.

Note that:

This command applies to configuring a non-user-defined remote ID sub-option only. After you configure the padding content for the remote ID sub-option using the **dhcp-snooping information remote-id string** command, ASCII is adopted as the code type.

Examples

Configure the code type for the non-user-defined remote ID sub-option as **ascii**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabiEthernet1/0/1] dhcp-snooping information remote-id format-type ascii
```

dhcp-snooping information remote-id string

Syntax

dhcp-snooping information [**vlan** *vlan-id*] **remote-id string** { *remote-id* | **sysname** }

undo dhcp-snooping information [**vlan** *vlan-id*] **remote-id string**

View

Layer 2 Ethernet port view

Default Level

2: System level

Parameters

vlan *vlan-id*: Specifies a VLAN ID, in the range of 1 to 4094.

remote-id: Padding content for the user-defined circuit ID sub-option, a case-sensitive string of 1 to 63 characters.

sysname: Specifies the device name as the padding content for the remote ID sub-option.

Description

Use the **dhcp-snooping information remote-id string** command to configure the padding content for the user-defined remote ID sub-option.

Use the **undo dhcp-snooping information remote-id string** command to restore the default.

By default, the padding content for the remote ID sub-option depends on the padding format of Option 82.

Note that:

- After you configure the padding content for the remote ID sub-option using this command, ASCII is adopted as the code type.
- If a VLAN is specified, the configured remote ID sub-option only takes effect within the VLAN; if no VLAN is specified, the configured remote ID sub-option takes effect in all VLANs. The former case has a higher priority; that is, the remote ID sub-option configured for a VLAN will be padded for the packets within the VLAN.

Related commands: **dhcp-snooping information format**.

Note

If you want to specify the character string **sysname** (a case-insensitive character string) as the padding content for the remote ID sub-option, you need to use quotation marks to make it take effect. For example, if you want to specify **Sysname** as the padding content for the remote ID sub-option, you need to enter the **dhcp relay information remote-id string** “Sysname” command.

Examples

Configure the padding content for the remote ID sub-option as **device001**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabiEthernet1/0/1] dhcp-snooping information remote-id string device001
```

dhcp-snooping information strategy

Syntax

dhcp-snooping information strategy { **drop** | **keep** | **replace** }

undo dhcp-snooping information strategy

View

Layer 2 Ethernet interface view

Default Level

2: System level

Parameters

drop: Drops the requesting message containing Option 82.

keep: Forwards the requesting message containing Option 82 without changing Option 82.

replace: Forwards the requesting message containing Option 82 after replacing the original Option 82 with the one padded in specified format.

Description

Use the **dhcp-snooping information strategy** command to configure the handling strategy for Option 82 in requesting messages.

Use the **undo dhcp-snooping information strategy command** to restore the default.

By default, the handling strategy for Option 82 in requesting messages is **replace**.

Examples

Configure the handling strategy for Option 82 in requesting messages as **keep**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabiEthernet1/0/1] dhcp-snooping information enable
[Sysname-GigabiEthernet1/0/1] dhcp-snooping information strategy keep
```

dhcp-snooping trust

Syntax

dhcp-snooping trust [**no-user-binding**]

undo dhcp-snooping trust

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

no-user-binding: Specifies the port not to record the clients' IP-to-MAC bindings in DHCP requests it receives. The command without this keyword records the IP-to-MAC bindings of clients.

Description

Use the **dhcp-snooping trust** command to configure a port as a trusted port.

Use the **undo dhcp-snooping trust** command to restore the default state of a port.

All ports are untrusted by default.

After enabling DHCP snooping, you need to specify the ports connected to the valid DHCP servers as trusted to ensure that DHCP clients can obtain valid IP addresses.

Related commands: **display dhcp-snooping trust**.

Examples

Specify GigabiEthernet 1/0/1 as a trusted port and enable it to record the IP-to-MAC bindings of clients.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabiEthernet1/0/1] dhcp-snooping trust
```

display dhcp-snooping

Syntax

display dhcp-snooping [**ip** *ip-address*]

View

Any view

Default Level

1: Monitor level

Parameters

ip *ip-address*: Displays the DHCP snooping entries corresponding to the specified IP address.

Description

Use the **display dhcp-snooping** command to display DHCP snooping entries.

Note

Only the DHCP snooping entries containing IP-to-MAC bindings that are present both in the DHCP-ACK and DHCP-REQUEST messages are displayed by using the **display dhcp-snooping** command.

Examples

Display all DHCP snooping entries.

```
<Sysname> display dhcp-snooping
 DHCP Snooping is enabled.
 The client binding table for all untrusted ports.
 Type : D--Dynamic , S--Static
 Type   IP Address      MAC Address      Lease       VLAN Interface
 ====  ===============  ===============  ==========  ==== =================
 D     10.1.1.1       00e0-fc00-0006   286           1     GigabiEthernet1/0/1
---   1 dhcp-snooping item(s) found   ---
```

Table 7-1 display dhcp snooping command output description

Field	Description
Type	Binding type
IP Address	IP address assigned to the DHCP client
MAC Address	MAC address of the DHCP client
Lease	Lease period left (in seconds)
VLAN	VLAN where the port connecting the DHCP client resides
Interface	Port to which the DHCP client is connected

display dhcp-snooping information

Syntax

display dhcp-snooping information { **all** | **interface** *interface-type interface-number* }

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays the Option 82 configuration information of all Layer 2 Ethernet interfaces.

interface *interface-type interface-number*: Displays the Option 82 configuration information of a specified interface.

Description

Use the **display dhcp-snooping information** command to display Option 82 configuration information on the DHCP snooping device.

Examples

Display the Option 82 configuration information of all interfaces.

```
<Sysname> display dhcp-snooping information all
Interface: GigabiEthernet 1/0/1
    Status: Enable
    Strategy: Replace
    Format: Verbose
    Circuit ID format-type: HEX
    Remote ID format-type: ASCII
    Node identifier: aabbcc
    User defined:
        Circuit ID: company001
Interface: GigabiEthernet 1/0/2
    Status: Disable
    Strategy: Keep
    Format: Normal
    Circuit ID format-type: HEX
    Remote ID format-type: ASCII
    User defined:
        Circuit ID: company001
        Remote ID: device001
        VLAN 10:
            Circuit ID: vlan10@company001
        VLAN 20:
            Remote ID: device001
```

display dhcp-snooping packet statistics

Syntax

display dhcp-snooping packet statistics [**slot** *slot-number*]

View

Any view

Default Level

1: Monitor level

Parameters

slot *slot-number*: Displays the DHCP packet statistics of the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

Description

Use the **display dhcp-snooping packet statistics** command to display DHCP packet statistics on the DHCP snooping device.

On a device in IRF, executing the **display dhcp-snooping packet statistics** command without the **slot** keyword only displays DHCP packet statistics on the device where the command is executed.

Examples

Display DHCP packet statistics on the DHCP snooping device.

```
<Sysname> display dhcp-snooping packet statistics
 DHCP packets received               : 100
 DHCP packets sent                   : 200
 Packets dropped due to rate limitation : 20
 Dropped invalid packets             : 0
```

display dhcp-snooping trust

Syntax

display dhcp-snooping trust

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display dhcp-snooping trust** command to display information about trusted ports.

Related commands: **dhcp-snooping trust**.

Examples

Display information about trusted ports.

```
<Sysname> display dhcp-snooping trust
 DHCP Snooping is enabled.
 DHCP Snooping trust becomes active.
 Interface                              Trusted
 =========================              ============
 GigabiEthernet1/0/1                     Trusted
```

The above output shows that DHCP snooping is enabled, DHCP snooping trust is active, and port GigabiEthernet 1/0/1 is trusted.

reset dhcp-snooping

Syntax

reset dhcp-snooping { **all** | **ip** *ip-address* }

View

User view

Default Level

1: Monitor level

Parameters

all: Clears all DHCP snooping entries.

ip *ip-address*: Clears the DHCP snooping entries of the specified IP address.

Description

Use the **reset dhcp-snooping** command to clear DHCP snooping entries.

For an IRF, DHCP snooping entries on all devices will be cleared after you execute this command.

Examples

Clear all DHCP snooping entries.

```
<Sysname> reset dhcp-snooping all
```

reset dhcp-snooping packet statistics

Syntax

reset dhcp-snooping packet statistics [**slot** *slot-number*]

View

User view

Default Level

2: System level

Parameters

slot *slot-number*: Clears the DHCP packet statistics of the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

Description

Use the **reset dhcp-snooping packet statistics** command to clear DHCP packet statistics on the DHCP snooping device.

On a device in IRF, executing the **reset dhcp-snooping packet statistics** command without the **slot** keyword only clears DHCP packet statistics on the device where the command is executed.

Examples

Clear DHCP packet statistics on the DHCP snooping device.

```
<Sysname> reset dhcp-snooping packet statistics
```

8 BOOTP Client Configuration Commands

Note

- BOOTP client configuration can only be used on VLAN interfaces.
- If several VLAN interfaces sharing the same MAC address obtain IP addresses through a BOOTP relay agent, the BOOTP server cannot be a Windows 2000 Server or Windows 2003 Server.
- You are not recommended to enable both the DHCP client and the DHCP snooping on the same device. Otherwise, DHCP snooping entries may fail to be generated, or the BOOTP client may fail to obtain an IP address.

BOOTP Client Configuration Commands

display bootp client

Syntax

display bootp client [**interface** *interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the BOOTP client information of the interface.

Description

Use the **display bootp client** command to display related information about a BOOTP client.

Note:

- If **interface** *interface-type interface-number* is not specified, the command will display information about BOOTP clients on all interfaces.
- If **interface** *interface-type interface-number* is specified, the command will display information about the BOOTP client on the specified interface.

Examples

Display related information of the BOOTP client on VLAN-interface 1.

```
<Sysname> display bootp client interface vlan-interface 1
```

```
Vlan-interface1 BOOTP client information:
Allocated IP: 169.254.0.2 255.255.0.0
Transaction ID = 0x3d8a7431
Mac Address  00e0-fc0a-c3ef
```

Table 8-1 display bootp client command output description

Field	Description
Vlan-interface1 BOOTP client information	Information of the interface serving as a BOOTP client
Allocated IP	BOOTP client's IP address allocated by the BOOTP server
Transaction ID	Value of the **XID** field in a BOOTP message, namely, a random number chosen while the BOOTP client sends a BOOTP request to the BOOTP server. It is used to match a response message from the BOOTP server. If the values of the **XID** field are different in the BOOTP response and request, the BOOTP client will drop the BOOTP response.
Mac Address	MAC address of a BOOTP client

ip address bootp-alloc

Syntax

ip address bootp-alloc

undo ip address bootp-alloc

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **ip address bootp-alloc** command to enable an interface to obtain an IP address through BOOTP.

Use the **undo ip address bootp-alloc** command to disable the interface from obtaining an IP address through BOOTP.

By default, an interface does not obtain an IP address through BOOTP.

Related commands: **display bootp client**.

Examples

Configure VLAN-interface 1 to obtain IP address through BOOTP protocol.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address bootp-alloc
```

9 DNS Configuration Commands

Note

This document only covers IPv4 DNS configuration commands. For introduction to IPv6 DNS configuration commands, refer to *IPv6 Basics Commands* in the *IP Services Volume*.

DNS Configuration Commands

display dns domain

Syntax

display dns domain [**dynamic**]

View

Any view

Default Level

1: Monitor level

Parameters

dynamic: Displays the domain name suffixes dynamically obtained through DHCP or other protocols.

Description

Use the **display dns domain** command to display the domain name suffixes.

Related commands: **dns domain**.

Examples

Display domain name suffixes.

```
<Sysname> display dns domain
 Type:
  D:Dynamic    S:Static

No.    Type   Domain-name
1      S      com
```

Table 9-1 display dns domain command output description

Field	Description
No	Sequence number
Type	Type of domain name suffix: S represents a statically configured domain name suffix, and D represents a domain name suffix obtained dynamically through DHCP.
Domain-name	Domain name suffix

display dns dynamic-host

Syntax

display dns dynamic-host

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display dns dynamic-host** command to display the information of the dynamic domain name resolution cache.

Examples

Display the information of the dynamic domain name resolution cache.

```
<Sysname> display dns dynamic-host
No. Host               IP Address          TTL
1   www.baidu.com       202.108.249.134     63000
2   www.yahoo.akadns.net  66.94.230.39       24
3   www.hotmail.com      207.68.172.239      3585
4   www.eyou.com        61.136.62.70        3591
```

Table 9-2 display dns dynamic-host command output description

Field	Description
No	Sequence number
Host	Domain name
IP Address	IP address for the corresponding domain name
TTL	Time that a mapping can be stored in the cache (in seconds).

Note

A domain name in the **display dns dynamic-host** command contains 21 characters at most. If a domain name consists of more than 21 characters, only the first 21 characters are displayed.

display dns server

Syntax

display dns server [**dynamic**]

View

Any view

Default Level

1: Monitor level

Parameters

dynamic: Displays the DNS server information dynamically obtained through DHCP or other protocols

Description

Use the **display dns server** command to display the DNS server information.

Related commands: **dns server**.

Examples

Display the DNS server information.

```
<Sysname> display dns server
Type:
  D:Dynamic    S:Static

DNS Server  Type  IP Address
   1      S     169.254.65.125
```

Table 9-3 display dns server command output description

Field	Description
DNS Server	Sequence number of the DNS server, configured automatically by the device, starting from 1.
Type	Type of domain name server: S represents a statically configured DNS server, and D represents a DNS server obtained dynamically through DHCP.
IP Address	IP address of the DNS server

display ip host

Syntax

display ip host

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ip host** command to display the host names and corresponding IP addresses in the static domain name resolution table.

Examples

Display the host names and corresponding IP addresses in the static domain name resolution table.

```
<Sysname> display ip host
Host           Age     Flags       Address
My         0       static      1.1.1.1
Aa         0       static      2.2.2.4
```

Table 9-4 display ip host command output description

Field	Description
Host	Host name
Age	Time to live. 0 means that the static mapping will never age out. You can only manually remove the static mappings between host names and IP addresses.
Flags	Indicates the mapping type. Static represents static domain name resolution.
Address	Host IP address

dns domain

Syntax

dns domain *domain-name*

undo dns domain [*domain-name*]

View

System view

Default Level

2: System level

Parameters

domain-name: Domain name suffix, consisting of character strings separated by a dot (for example, aabbcc.com). Each separated string contains no more than 63 characters. A domain name suffix may include case-insensitive letters, digits, hyphens (-), underscores (_), and dots (.), with a total length of 238 characters.

Description

Use the **dns domain** command to configure a domain name suffix. The system can automatically add the suffix to part of the domain name you entered for resolution.

Use the **undo dns domain** command to delete a domain name suffix (with a domain name suffix specified) or all domain name suffixes (with no domain name suffix specified).

No domain name suffix is configured by default, that is, only the provided domain name is resolved.

You can configure a maximum of 10 domain name suffixes.

Related commands: **display dns domain**.

Examples

Configure com as a DNS suffix.

```
<Sysname> system-view
[Sysname] dns domain com
```

dns proxy enable

Syntax

dns proxy enable

undo dns proxy enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **dns proxy enable** command to enable DNS proxy.

Use the **undo dns proxy enable** command to disable DNS proxy.

By default, DNS proxy is disabled.

Examples

Enable DNS proxy.

```
<Sysname> system-view
[Sysname] dns proxy enable
```

dns resolve

Syntax

dns resolve

undo dns resolve

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **dns resolve** command to enable dynamic domain name resolution.

Use the **undo dns resolve** command to disable dynamic domain name resolution.

Dynamic domain name resolution is disabled by default.

Examples

Enable dynamic domain name resolution.

```
<Sysname> system-view
[Sysname] dns resolve
```

dns server

Syntax

dns server *ip-address*

undo dns server [*ip-address*]

View

System view

Default Level

2: System level

Parameters

ip-address: IP address of the DNS server.

Description

Use the **dns server** command to specify a DNS server.

Use the **undo dns server** to remove DNS server(s).

No DNS server is specified by default.

You can configure a maximum of six DNS servers, including those with IPv6 addresses.

Related commands: **display dns server**.

Examples

Specify the DNS server 172.16.1.1.

```
<Sysname> system-view
[Sysname] dns server 172.16.1.1
```

ip host

Syntax

ip host *hostname ip-address*

undo ip host *hostname* [*ip-address*]

View

System view

Default Level

2: System level

Parameters

hostname: Host name, consisting of 1 to 20 characters, including case-insensitive letters, numbers, hyphens (-), underlines (_), or dots (.). The host name must include at least one letter.

ip-address: IP address of the specified host in dotted decimal notation.

Description

Use the **ip host** command to create a host name to IP address mapping in the static resolution table.

Use the **undo ip host** command to remove a mapping.

No mappings are created by default.

You can configure only one mapping for a host name. A mapping newly configured for the host name will overwrite the previous one if there is any.

Related commands: **display ip host**.

Examples

Map the IP address 10.110.0.1 to the host name aaa.

```
<Sysname> system-view
[Sysname] ip host aaa 10.110.0.1
```

reset dns dynamic-host

Syntax

reset dns dynamic-host

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **reset dns dynamic-host** command to clear the dynamic domain name resolution information.

Related commands: **display dns dynamic-host**.

Examples

Clear the dynamic domain name resolution information.

```
<Sysname> reset dns dynamic-host
```

10 IP Performance Optimization Configuration Commands

IP Performance Optimization Configuration Commands

display fib

Syntax

display fib [**|** { **begin** | **include** | **exclude** } *regular-expression* | **acl** *acl-number* | **ip-prefix** *ip-prefix-name*]

View

Any view

Default Level

1: Monitor level

Parameters

|: Uses a regular expression to match FIB entries. For detailed information about regular expression, refer to CLI display in *Basic System Configuration* in the *System Volume*.

begin: Displays the first entry that matches the specified regular expression and all the FIB entries following it.

exclude: Displays the FIB entries that do not match the specified regular expression.

include: Displays the FIB entries that match the specified regular expression.

regular-expression: A case-sensitive string of 1 to 256 characters, excluding spaces.

acl *acl-number*: Displays FIB entries matching a specified ACL numbered from 2000 to 2999. If the specified ACL does not exist, all FIB entries are displayed.

ip-prefix *ip-prefix-name*: Displays FIB entries matching a specified IP prefix list, a string of 1 to 19 characters. If the specified IP prefix list does not exist, all FIB entries are displayed.

Description

Use the **display fib** command to display FIB entries. If no parameters are specified, all FIB entries will be displayed.

Examples

Display all FIB entries.

```
<Sysname> display fib
Destination count: 4    FIB entry count: 4

Flag:
```

```
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay

Destination/Mask  Nexthop    Flag    OutInterface  InnerLabel Token
10.2.0.0/16      10.2.1.1    U       VLAN1        Null      Invalid
10.2.1.1/32      127.0.0.1   UH      InLoop0      Null      Invalid
127.0.0.0/8      127.0.0.1   U       InLoop0      Null      Invalid
127.0.0.1/32     127.0.0.1   UH      InLoop0      Null      Invalid
```

Display FIB information passing ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.2.0.0 0.0.255.255
[Sysname-acl-basic-2000] display fib acl 2000
Destination count: 2   FIB entry count: 2

 Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay

Destination/Mask  Nexthop    Flag    OutInterface  InnerLabel Token
10.2.0.0/16      10.2.1.1    U      VLAN1        Null      Invalid
10.2.1.1/32      127.0.0.1    UH     InLoop0      Null      Invalid
```

Display all entries that contain the string **127** and start from the first one.

```
<Sysname> display fib | begin 127
Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay

Destination/Mask  Nexthop    Flag    OutInterface  InnerLabel Token
10.2.1.1/32      127.0.0.1   UH      InLoop0      Null      Invalid
127.0.0.0/8      127.0.0.1   U       InLoop0      Null      Invalid
127.0.0.1/32     127.0.0.1   UH      InLoop0      Null      Invalid
```

Display FIB information passing the IP prefix list **abc0**.

```
<Sysname> system-view
[Sysname] ip ip-prefix abc0 permit 10.2.0.0 16
[Sysname] display fib ip-prefix abc0
Destination count: 1   FIB entry count: 1

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay

Destination/Mask Nexthop    Flag    OutInterface  InnerLabel Token
10.2.0.0/16     10.2.1.1    U       VLAN1        Null      Invalid
```

Table 10-1 display fib command output description

Field	Description
Destination count	Total number of destination addresses
FIB entry count	Total number of FIB entries
Destination/Mask	Destination address/length of mask
Nexthop	Address of next hop
Flag	Flags of routes: • “U”—Usable route • “G”—Gateway route • “H”—Host route • “B”—Blackhole route • “D”—Dynamic route • “S”—Static route • “R”—Relay route
OutInterface	Outbound interface
InnerLabel	Inner label
Token	LSP index number

display fib *ip-address*

Syntax

display fib *ip-address* [*mask* | *mask-length*]

View

Any view

Default Level

1: Monitor level

Parameters

ip-address: Destination IP address, in dotted decimal notation.

mask: IP address mask.

mask-length: Length of IP address mask.

Description

Use the **display fib** *ip-address* command to display FIB entries that match the specified destination IP address.

If no mask or mask length is specified, the FIB entry that matches the destination IP address and has the longest mask will be displayed; if the mask is specified, the FIB entry that exactly matches the specified destination IP address will be displayed.

Examples

Display the FIB entries that match the destination IP address of 10.2.1.1.

```
<Sysname> display fib 10.2.1.1
Destination count: 1    FIB entry count: 1

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Relay

Destination/Mask  Nexthop     Flag     OutInterface  InnerLabel Token
10.2.1.1/32       127.0.0.1   UH       InLoop0       Null       Invalid
```

For description about the above output, refer to Table 10-1.

display icmp statistics

Syntax

display icmp statistics [**slot** *slot-number*]

View

Any view

Default Level

1: Monitor level

Parameters

slot *slot-number*: Displays the ICMP statistics on the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

Description

Use the **display icmp statistics** command to display ICMP statistics.

Related commands: **display ip interface** (in *IP Addressing Commands* of the *IP Services Volume*), **reset ip statistics**.

Examples

Display ICMP statistics.

```
<Sysname> display icmp statistics
  Input: bad formats   0               bad checksum          0
         echo          5               destination unreachable 0
         source quench 0               redirects             0
         echo reply    10              parameter problem     0
         timestamp     0               information request   0
         mask requests 0               mask replies          0
         time exceeded 0
  Output:echo          10              destination unreachable 0
         source quench 0               redirects             0
         echo reply    5               parameter problem     0
         timestamp     0               information reply     0
         mask requests 0               mask replies          0
```

```
time exceeded 0
```

Table 10-2 display icmp statistics command output description

Field	Description
bad formats	Number of input wrong format packets
bad checksum	Number of input wrong checksum packets
echo	Number of input/output echo packets
destination unreachable	Number of input/output destination unreachable packets
source quench	Number of input/output source quench packets
redirects	Number of input/output redirection packets
echo reply	Number of input/output replies
parameter problem	Number of input/output parameter problem packets
timestamp	Number of input/output time stamp packets
information request	Number of input information request packets
mask requests	Number of input/output mask requests
mask replies	Number of input/output mask replies
information reply	Number of output information reply packets
time exceeded	Number of input/output expiration packets

display ip socket

Syntax

display ip socket [**socktype** *sock-type*] [*task-id socket-id*] [**slot** *slot-number*]

View

Any view

Default Level

1: Monitor level

Parameters

socktype *sock-type*: Displays the socket information of this type. The sock type is in the range 1 to 3, corresponding to TCP, UDP and raw IP respectively.

task-id: Displays the socket information of this task. Task ID is in the range 1 to 100.

socket-id: Displays the information of the socket. Socket ID is in the range 0 to 3072.

slot *slot-number*: Displays the socket information of the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

Description

Use the **display ip socket** command to display socket information.

Examples

Display the TCP socket information.

```
<Sysname> display ip socket
SOCK_STREAM:
Task = VTYD(38), socketid = 1, Proto = 6,
LA = 0.0.0.0:23, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_REUSEPORT SO_SENDVPNID(3073) SO_SETKEEPALIVE,
socket state = SS_PRIV SS_ASYNC

Task = HTTP(36), socketid = 1, Proto = 6,
LA = 0.0.0.0:80, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT,
socket state = SS_PRIV SS_NBIO

Task = ROUT(69), socketid = 10, Proto = 6,
LA = 0.0.0.0:179, FA = 192.168.1.45:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEADDR SO_REUSEPORT SO_SENDVPNID(0),
socket state = SS_PRIV SS_ASYNC

Task = VTYD(38), socketid = 4, Proto = 6,
LA = 192.168.1.40:23, FA = 192.168.1.52:1917,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 237, rb_cc = 0,
socket option = SO_KEEPALIVE SO_OOBINLINE SO_REUSEPORT SO_SENDVPNID(0) SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

Task = VTYD(38), socketid = 3, Proto = 6,
LA = 192.168.1.40:23, FA = 192.168.1.84:1503,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_KEEPALIVE SO_OOBINLINE SO_REUSEPORT SO_SENDVPNID(0) SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

Task = ROUT(69), socketid = 11, Proto = 6,
LA = 192.168.1.40:1025, FA = 192.168.1.45:179,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEADDR SO_LINGER SO_SENDVPNID(0),
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

SOCK_DGRAM:
Task = NTPT(37), socketid = 1, Proto = 17,
LA = 0.0.0.0:123, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM SO_SENDVPNID(3073),
socket state = SS_PRIV
```

```
Task = AGNT(51), socketid = 1, Proto = 17,
LA = 0.0.0.0:161, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM SO_SENDVPNID(3073),
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = RDSO(56), socketid = 1, Proto = 17,
LA = 0.0.0.0:1024, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV

Task = TRAP(52), socketid = 1, Proto = 17,
LA = 0.0.0.0:1025, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 0, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV

Task = RDSO(56), socketid = 2, Proto = 17,
LA = 0.0.0.0:1812, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV

SOCK_RAW:
Task = ROUT(69), socketid = 8, Proto = 89,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 262144, rcvbuf = 262144, sb_cc = 0, rb_cc = 0,
socket option = SO_SENDVPNID(0) SO_RCVVPNID(0),
socket state = SS_PRIV SS_ASYNC

Task = ROUT(69), socketid = 3, Proto = 2,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 32767, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
socket option = SO_SENDVPNID(0) SO_RCVVPNID(0),
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = ROUT(69), socketid = 2, Proto = 103,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 65536, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
socket option = SO_SENDVPNID(0) SO_RCVVPNID(0),
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = ROUT(69), socketid = 1, Proto = 65,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 32767, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
socket option = 0,
```

```
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = RSVP(73), socketid = 1, Proto = 46,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 4194304, rcvbuf = 4194304, sb_cc = 0, rb_cc = 0,
socket option = 0,
socket state = SS_PRIV SS_NBIO SS_ASYNC
```

Table 10-3 display ip socket command output description

Field	Description
SOCK_STREAM	TCP socket
SOCK_DGRAM	UDP socket
SOCK_RAW	Raw IP socket
Task	Task number
socketid	Socket ID
Proto	Protocol number of the socket, indicating the protocol type that IP carries
LA	Local address and local port number
FA	Remote address and remote port number
sndbuf	Sending buffer size of the socket, in bytes
rcvbuf	Receiving buffer size of the socket, in bytes
sb_cc	Current data size in the sending buffer (It is available only for TCP that can buffer data)
rb_cc	Data size currently in the receiving buffer
socket option	Socket option
socket state	Socket state

display ip statistics

Syntax

display ip statistics [**slot** *slot-number*]

View

Any view

Default Level

1: Monitor level

Parameters

slot *slot-number*: Displays statistics of IP packets on the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

Description

Use the **display ip statistics** command to display statistics of IP packets.

Related commands: **display ip interface** (in *IP Addressing Commands* of the *IP Services Volume*), **reset ip statistics**.

Examples

Display statistics of IP packets.

```
<Sysname> display ip statistics
  Input:   sum          7120          local          112
          bad protocol   0            bad format      0
          bad checksum   0            bad options     0
  Output:  forwarding    0            local           27
          dropped       0            no route        2
          compress fails 0
  Fragment:input         0            output          0
          dropped       0
          fragmented     0            couldn't fragment 0
  Reassembling:sum       0            timeouts        0
```

Table 10-4 display ip statistics command output description

Field		Description
Input:	sum	Total number of packets received
	local	Total number of packets with destination being local
	bad protocol	Total number of unknown protocol packets
	bad format	Total number of packets with incorrect format
	bad checksum	Total number of packets with incorrect checksum
	bad options	Total number of packets with incorrect option
Output:	forwarding	Total number of packets forwarded
	local	Total number of packets sent from the local
	dropped	Total number of packets discarded
	no route	Total number of packets for which no route is available
	compress fails	Total number of packets failed to be compressed
Fragment:	input	Total number of fragments received
	output	Total number of fragments sent
	dropped	Total number of fragments dropped
	fragmented	Total number of packets successfully fragmented
	couldn't fragment	Total number of packets that failed to be fragmented
Reassembling	sum	Total number of packets reassembled
	timeouts	Total number of reassembly timeout fragments

display tcp statistics

Syntax

display tcp statistics

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display tcp statistics** command to display statistics of TCP traffic.

Related commands: **display tcp status**, **reset tcp statistics**.

Examples

Display statistics of TCP traffic.

```
<Sysname> display tcp statistics
Received packets:
    Total: 8457
    packets in sequence: 3660 (5272 bytes)
    window probe packets: 0, window update packets: 0
    checksum error: 0, offset error: 0, short error: 0

    duplicate packets: 1 (8 bytes), partially duplicate packets: 0 (0 bytes)
    out-of-order packets: 17 (0 bytes)
    packets of data after window: 0 (0 bytes)
    packets received after close: 0

    ACK packets: 4625 (141989 bytes)
    duplicate ACK packets: 1702, too much ACK packets: 0

Sent packets:
    Total: 6726
    urgent packets: 0
    control packets: 21 (including 0 RST)
    window probe packets: 0, window update packets: 0

    data packets: 6484 (141984 bytes) data packets retransmitted: 0 (0 bytes)
    ACK-only packets: 221 (177 delayed)

Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 1682, keepalive probe: 1682, Keepalive timeout, so connections
disconnected : 0
```

```
Initiated connections: 0, accepted connections: 22, established connections: 22
Closed connections: 49 (dropped: 0, initiated dropped: 0)
Packets dropped with MD5 authentication: 0
Packets permitted with MD5 authentication: 0
```

Table 10-5 display tcp statistics command output description

Field		Description
Received packets:	Total	Total number of packets received
	packets in sequence	Number of packets arriving in sequence
	window probe packets	Number of window probe packets received
	window update packets	Number of window update packets received
	checksum error	Number of checksum error packets received
	offset error	Number of offset error packets received
	short error	Number of received packets with length being too small
	duplicate packets	Number of completely duplicate packets received
	partially duplicate packets	Number of partially duplicate packets received
	out-of-order packets	Number of out-of-order packets received
	packets of data after window	Number of packets outside the receiving window
	packets received after close	Number of packets that arrived after connection is closed
	ACK packets	Number of ACK packets received
	duplicate ACK packets	Number of duplicate ACK packets received
	too much ACK packets	Number of ACK packets for data unsent
Sent packets:	Total	Total number of packets sent
	urgent packets	Number of urgent packets sent
	control packets	Number of control packets sent
	window probe packets	Number of window probe packets sent; in the brackets are resent packets
	window update packets	Number of window update packets sent
	data packets	Number of data packets sent
	data packets retransmitted	Number of data packets retransmitted
	ACK-only packets	Number of ACK packets sent; in brackets are delayed ACK packets
Retransmitted timeout		Number of retransmission timer timeouts
connections dropped in retransmitted timeout		Number of connections broken due to retransmission timeouts
Keepalive timeout		Number of keepalive timer timeouts
keepalive probe		Number of keepalive probe packets sent
Keepalive timeout, so connections disconnected		Number of connections broken due to timeout of the keepalive timer

Field	Description
Initiated connections	Number of connections initiated
accepted connections	Number of connections accepted
established connections	Number of connections established
Closed connections	Number of connections closed; in brackets are connections closed accidentally (before receiving SYN from the peer) and connections closed initiatively (after receiving SYN from the peer)
Packets dropped with MD5 authentication	Number of packets dropped by MD5 authentication
Packets permitted with MD5 authentication	Number of packets permitted by MD5 authentication

display tcp status

Syntax

display tcp status

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display tcp status** command to display status of all TCP connections for monitoring TCP connections.

Examples

Display status of all TCP connections.

```
<Sysname> display tcp status
*: TCP MD5 Connection
TCPCB          Local Add:port       Foreign Add:port     State
03e37dc4       0.0.0.0:4001         0.0.0.0:0            Listening
04217174       100.0.0.204:23       100.0.0.253:65508    Established
```

Table 10-6 display tcp status command output description

Field	Description
*	If the status information of a TCP connection contains *, the TCP adopts the MD5 algorithm for authentication.
TCPCB	TCP control block
Local Add:port	Local IP address and port number
Foreign Add:port	Remote IP address and port number

Field	Description
State	State of the TCP connection

display udp statistics

Syntax

display udp statistics

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display udp statistics** command to display statistics of UDP packets.

Related commands: **reset udp statistics**.

Examples

Display statistics of UDP packets.

```
<Sysname> display udp statistics
Received packets:
    Total: 0
    checksum error: 0
    shorter than header: 0, data length larger than packet: 0
    unicast(no socket on port): 0
    broadcast/multicast(no socket on port): 0
    not delivered, input socket full: 0
    input packets missing pcb cache: 0
Sent packets:
    Total: 0
```

Table 10-7 display udp statistics command output description

Field		Description
Received packets:	Total	Total number of UDP packets received
	checksum error	Total number of packets with incorrect checksum
	shorter than header	Number of packets with data shorter than head
	data length larger than packet	Number of packets with data longer than packet
	unicast(no socket on port)	Number of unicast packets with no socket on port

Field		Description
	broadcast/multicast(no socket on port)	Number of broadcast/multicast packets without socket on port
	not delivered, input socket full	Number of packets not delivered to an upper layer due to a full socket cache
	input packets missing pcb cache	Number of packets without matching protocol control block (PCB) cache
Sent packets:	Total	Total number of UDP packets sent

ip forward-broadcast (interface view)

Syntax

ip forward-broadcast [**acl** *acl-number*]

undo ip forward-broadcast

View

Interface view

Default Level

2: System level

Parameters

acl *acl-number*: Access control list number, in the range 2000 to 3999. From 2000 to 2999 are numbers for basic ACLs, and from 3000 to 3999 are numbers for advanced ACLs. Only directed broadcasts permitted by the ACL can be forwarded.

Description

Use the **ip forward-broadcast** command to enable the interface to forward directed broadcasts to a directly-connected network.

Use the **undo ip forward-broadcast** command to disable the interface from forwarding directed broadcasts to a directly-connected network.

By default, an interface is disabled from forwarding directed broadcasts to a directly-connected network.

Examples

Enable VLAN-interface 2 to forward the directed broadcasts to a directly-connected network matching ACL 2001.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip forward-broadcast acl 2001
```

ip forward-broadcast (system view)

Syntax

ip forward-broadcast

undo ip forward-broadcast

View

System view

Default Level

1: Monitor level

Parameters

None

Description

Use the **ip forward-broadcast** command to enable the device to receive directed broadcasts.

Use the **undo ip forward-broadcast** command to disable the device from receiving directed broadcasts.

By default, the device is disabled from receiving directed broadcasts.

Examples

Enable the device to receive directed broadcasts.

```
<Sysname> system-view
[Sysname] ip forward-broadcast
```

ip redirects enable

Syntax

ip redirects enable

undo ip redirects

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **ip redirects enable** command to enable sending of ICMP redirection packets.

Use the **undo ip redirects** command to disable sending of ICMP redirection packets.

This feature is disabled by default.

Examples

Enable sending of ICMP redirect packets.

```
<Sysname> system-view
[Sysname] ip redirects enable
```

ip ttl-expires enable

Syntax

ip ttl-expires enable

undo ip ttl-expires

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **ip ttl-expires enable** command to enable the sending of ICMP timeout packets.

Use the **undo ip ttl-expires** command to disable sending ICMP timeout packets.

Sending ICMP timeout packets is enabled by default.

If the feature is disabled, the device will not send TTL timeout ICMP packets, but still send “reassembly timeout” ICMP packets.

Examples

Disable sending ICMP timeout packets.

```
<Sysname> system-view
[Sysname] undo ip ttl-expires
```

ip unreachables enable

Syntax

ip unreachables enable

undo ip unreachables

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **ip unreachables enable** command to enable the sending of ICMP destination unreachable packets.

Use the **undo ip unreachables** command to disable sending ICMP destination unreachable packets.

Sending ICMP destination unreachable packets is disabled by default.

Examples

Enable sending ICMP destination unreachable packets.

```
<Sysname> system-view
[Sysname] ip unreachables enable
```

reset ip statistics

Syntax

reset ip statistics [**slot** *slot-number*]

View

User view

Default Level

2: System level

Parameters

slot *slot-number*: Clears IP packet statistics on the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

Description

Use the **reset ip statistics** command to clear statistics of IP packets.

Related commands: **display ip interface** (in *IP Addressing Commands* of the *IP Services Volume*), **display ip statistics**.

Examples

Clear statistics of IP packets.

```
<Sysname> reset ip statistics
```

reset tcp statistics

Syntax

reset tcp statistics

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **reset tcp statistics** command to clear statistics of TCP traffic.

Related commands: **display tcp statistics**.

Examples

Display statistics of TCP traffic.

```
<Sysname> reset tcp statistics
```

reset udp statistics

Syntax

reset udp statistics

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **reset udp statistics** command to clear statistics of UDP traffic.

Examples

Display statistics of UDP traffic.

```
<Sysname> reset udp statistics
```

tcp timer fin-timeout

Syntax

tcp timer fin-timeout *time-value*

undo tcp timer fin-timeout

View

System view

Default Level

2: System level

Parameters

time-value: Length of the TCP finwait timer in seconds, in the range 76 to 3,600.

Description

Use the **tcp timer fin-timeout** command to configure the length of the TCP finwait timer.

Use the **undo tcp timer fin-timeout** command to restore the default.

By default, the length of the TCP finwait timer is 675 seconds.

Note that the actual length of the finwait timer is determined by the following formula:

Actual length of the finwait timer = (Configured length of the finwait timer – 75) + configured length of the synwait timer

Related commands: **tcp timer syn-timeout**, **tcp window**.

Examples

Set the length of the TCP finwait timer to 800 seconds.

```
<Sysname> system-view
[Sysname] tcp timer fin-timeout 800
```

tcp timer syn-timeout

Syntax

tcp timer syn-timeout *time-value*

undo tcp timer syn-timeout

View

System view

Default Level

2: System level

Parameters

time-value: TCP finwait timer in seconds, in the range 2 to 600.

Description

Use the **tcp timer syn-timeout** command to configure the length of the TCP synwait timer.

Use the **undo tcp timer syn-timeout** command to restore the default.

By default, the value of the TCP synwait timer is 75 seconds.

Related commands: **tcp timer fin-timeout**, **tcp window**.

Examples

Set the length of the TCP synwait timer to 80 seconds.

```
<Sysname> system-view
```

```
[Sysname] tcp timer syn-timeout 80
```

tcp window

Syntax

tcp window *window-size*

undo tcp window

View

System view

Default Level

2: System level

Parameters

window-size: Size of the send/receive buffer in KB, in the range 1 to 32.

Description

Use the **tcp window** command to configure the size of the TCP send/receive buffer.

Use the **undo tcp window** command to restore the default.

The size of the TCP send/receive buffer is 8 KB by default.

Related commands: **tcp timer fin-timeout**, **tcp timer syn-timeout**.

Examples

Configure the size of the TCP send/receive buffer as 3 KB.

```
<Sysname> system-view
[Sysname] tcp window 3
```

11 UDP Helper Configuration Commands

UDP Helper Configuration Commands

display udp-helper server

Syntax

display udp-helper server [**interface** *interface-type interface-number*]

View

Any view

Default Level

2: System level

Parameters

interface *interface-type interface-number*: Displays information of forwarded UDP packets on the specified interface.

Description

Use the **display udp-helper server** command to display the information of forwarded UDP packets on the specified interface or all interfaces.

If *interface-type interface-number* is not specified, this command displays the information of forwarded UDP packets on all interfaces.

Examples

Display the information of forwarded UDP packets on the interface VLAN-interface 1.

```
<Sysname> display udp-helper server interface vlan-interface 1
Interface name     Server address       Packets sent
Vlan-interface1        192.1.1.2            0
```

The information above shows that the IP address of the destination server corresponding to the interface VLAN-interface 1 is 192.1.1.2, and that no packets are forwarded to the destination server.

reset udp-helper packet

Syntax

reset udp-helper packet

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **reset udp-helper packet** command to clear the statistics of UDP packets forwarded.

Related commands: **display udp-helper server**.

Examples

Clear the statistics of the forwarded UDP packets.

```
<Sysname> reset udp-helper packet
```

udp-helper enable

Syntax

udp-helper enable

undo udp-helper enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **udp-helper enable** command to enable UDP Helper. The device enabled with UDP Helper functions as a relay agent that converts UDP broadcast packets into unicast packets and forwards them to a specified destination server.

Use the **undo udp-helper enable** command to disable UDP Helper.

By default, UDP Helper is disabled.

Examples

Enable UDP Helper

```
<Sysname> system-view
[Sysname] udp-helper enable
```

udp-helper port

Syntax

udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

undo udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

View

System view

Default Level

2: System level

Parameters

port-number: UDP port number with which packets need to be forwarded, in the range of 1 to 65535 (except 67 and 68).

dns: Forwards DNS data packets. The corresponding UDP port number is 53.

netbios-ds: Forwards NetBIOS data packets. The corresponding UDP port number is 138.

netbios-ns: Forwards NetBIOS name service data packets. The corresponding UDP port number is 137.

tacacs: Forwards terminal access controller access control system (TACACS) data packet. The corresponding UDP port number is 49.

tftp: Forwards TFTP data packets. The corresponding UDP port number is 69.

time: Forwards time service data packets. The corresponding UDP port number is 37.

Description

Use the **udp-helper port** command to enable the forwarding of packets with the specified UDP port number.

Use the **undo udp-helper port** command to remove the configured UDP port numbers.

By default, no UDP port number is specified.

The specified UDP port numbers will all be removed if UDP Helper is disabled.

Examples

Forward broadcast packets with the UDP destination port number 100.

```
<Sysname> system-view
[Sysname] udp-helper port 100
```

udp-helper server

Syntax

udp-helper server *ip-address*

undo udp-helper server [*ip-address*]

View

Interface view

Default Level

2: System level

Parameters

ip-address: IP address of the destination server, in dotted decimal notation.

Description

Use the **udp-helper server** command to specify the destination server which UDP packets need to be forwarded to.

Use the **undo udp-helper server** command to remove the destination server.

No destination server is configured by default.

Currently, you can configure up to 20 destination servers on an interface.

Note that you will remove all the destination servers on an interface if you carry out the **undo udp-helper server** command without the *ip-address* argument.

Related commands: **display udp-helper server**.

Examples

Specify the IP address of the destination server as 192.1.1.2 on the interface VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] udp-helper server 192.1.1.2
```

12 IPv6 Basics Configuration Commands

IPv6 Basics Configuration Commands

display dns ipv6 dynamic-host

Syntax

display dns ipv6 dynamic-host

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display dns ipv6 dynamic-host** command to display IPv6 dynamic domain name information, including the domain name, IPv6 address, and TTL of the DNS entries.

You can use the **reset dns ipv6 dynamic-host** command to clear all IPv6 dynamic domain name information from the cache.

Examples

Display IPv6 dynamic domain name information.

```
<Sysname> display dns ipv6 dynamic-host
NoHost             IPv6 Address     TTL
1     aaa              2001::2          6
```

Table 12-1 display dns ipv6 dynamic-host command output description

Field	Description
No	Sequence number
Host	Host name
IPv6 address	IPv6 address of the host
TTL	Time within which an entry can be cached, in seconds

Note

For a domain name displayed with the **display dns ipv6 dynamic-host** command, no more than 21 characters can be displayed. If the domain name exceeds the maximum length, the first 21 characters will be displayed.

display dns ipv6 server

Syntax

display dns ipv6 server [**dynamic**]

View

Any view

Default Level

1: Monitor level

Parameters

dynamic: Displays IPv6 DNS server information acquired dynamically through DHCP or other protocols.

Description

Use the **display dns ipv6 server** command to display IPv6 DNS server information.

Examples

Display IPv6 DNS server information.

```
<Sysname> display dns ipv6 server
 Type:
  D:Dynamic    S:Static

DNS Server  Type  IPv6 Address                              (Interface Name)
    1       S     1::1
    2       S     FE80:1111:2222:3333:4444:5555:6666:7777  Vlan2
```

Table 12-2 display dns ipv6 server command output description

Field	Description
DNS Server	Sequence number of the DNS server, which is assigned automatically by the system, starting from 1.
Type	Type of the DNS server: “S” represents a statically configured DNS server, and “D” represents a DNS server obtained dynamically through DHCP.
IPv6 Address	IPv6 address of the DNS server
Interface Name	Interface name, which is available only for a DNS server with an IPv6 link-local address configured.

display ipv6 fib

Syntax

display ipv6 fib [*slot-number*] [*ipv6-address*]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-address: Displays the IPv6 FIB entries for an IPv6 address.

slot-number: Displays the IPv6 forwarding information base (FIB) entries of a specified device in an IRF. If no IRF is formed, the IPv6 FIB entries of the current device are displayed only. The *slot-number* argument indicates the member ID of the device.

Description

Use the **display ipv6 fib** command to display IPv6 FIB entries. If no argument is specified, all IPv6 FIB entries will be displayed.

The device looks up a matching IPv6 FIB entry for forwarding an IPv6 packet.

Examples

Display all IPv6 FIB entries.

```
<Sysname> display ipv6 fib
FIB Table:
 Total number of Routes : 1

 Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static

Destination:    ::1                              PrefixLength : 128
NextHop    :    ::1                              Flag         : HU
Label      :    NULL                             Tunnel ID    : 0
TimeStamp  :    Date- 7/14/2008, Time- 15:17:15
Interface  :    InLoopBack0
```

Table 12-3 display ipv6 fib command output description

Field	Description
Total number of Routes	Total number of routes in the FIB
Destination	Destination address
PrefixLength	Prefix length of the destination address
NextHop	Next hop

Field	Description
Flag	Route flag: • U — Usable route • G — Gateway route • H — Host route • B — Black hole route • D — Dynamic route • S — Static route
Label	Label
Tunnel ID	ID of a tunnel
TimeStamp	Generation time of a FIB entry
Interface	Outgoing interface

display ipv6 host

Syntax

display ipv6 host

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ipv6 host** command to display the mappings between host names and IPv6 addresses in the static domain name resolution table.

Related commands: **ipv6 host**.

Examples

Display the mappings between host names and IPv6 addresses in the static domain name resolution table.

```
<Sysname> display ipv6 host
Host              Age         Flags         IPv6Address
aaa               0           static         2002::1
bbb               0           static         2002::2
```

Table 12-4 display ipv6 host command output description

Field	Description
Host	Host name
Age	Time for the entry to live. “0” is displayed in the case of static configuration.

Field	Description
Flags	Flag indicating the type of mapping between a host name and an IPv6 address. Static indicates a static mapping.
IPv6Address	IPv6 address of a host

display ipv6 interface

Syntax

display ipv6 interface [*interface-type* [*interface-number*]] [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type: Interface type.

interface-number: Interface number.

verbose: Displays the detailed IPv6 information of an interface.

Description

Use the **display ipv6 interface** command to display the IPv6 information of an interface for which an IPv6 address can be configured.

If *interface-type interface-number* is not specified, the IPv6 information of all interfaces for which IPv6 addresses can be configured is displayed; if only *interface-type* is specified, the IPv6 information of the interfaces of the specified type for which IPv6 addresses can be configured is displayed; if *interface-type interface-number* is specified, the IPv6 information of the specified interface is displayed. If the **verbose** keyword is also specified, the detailed IPv6 information of the interface is displayed.

Note that:

Examples

Display the IPv6 information of VLAN-interface 2.

```
<Sysname> display ipv6 interface vlan-interface 2 verbose
Vlan-interface2 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::1234:56FF:FE65:4322
  Global unicast address(es):
    2001::1, subnet is 2001::/64
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF65:4322
    FF02::2
    FF02::1
```

```
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
IPv6 Packet statistics:
  InReceives:                0
  InTooShorts:               0
  InTruncatedPkts:           0
  InHopLimitExceeds:         0
  InBadHeaders:              0
  InBadOptions:              0
  ReasmReqds:                0
  ReasmOKs:                  0
  InFragDrops:               0
  InFragTimeouts:            0
  OutFragFails:              0
  InUnknownProtos:           0
  InDelivers:                0
  OutRequests:               0
  OutForwDatagrams:          0
  InNoRoutes:                0
  InTooBigErrors:            0
  OutFragOKs:                0
  OutFragCreates:            0
  InMcastPkts:               0
  InMcastNotMembers:         0
  OutMcastPkts:              0
  InAddrErrors:              0
  InDiscards:                0
  OutDiscards:               0
```

Table 12-5 display ipv6 interface verbose command output description (on a switch)

Field	Description
Vlan-interface2 current state	Physical state of the interface: • Administratively DOWN: Indicates that the VLAN interface is administratively down; that is, the interface is shut down using the **shutdown** command. • DOWN: Indicates that the VLAN interface is administratively up but its physical state is down; that is, no ports in the VLAN are up, which may be caused by a connection or link failure. • UP: Indicates that the administrative and physical states of the VLAN interface are both up.
Line protocol current state	Link layer protocol state of the interface: • DOWN: Indicates that the link layer protocol state of the VLAN interface is down, generally because no IP address is configured. • UP: Indicates that the link layer protocol state of the VLAN interface is up.

Field	Description
IPv6 is enabled	IPv6 packet forwarding state of the interface (after an IPv6 address is configured for an interface, IPv6 is automatically enabled on it; IPv6 packet forwarding is enabled in the example)
link-local address	Link-local address configured for the interface
Global unicast address(es)	Aggregatable global unicast address(es) configured for the interface
Joined group address(es)	Address(es) of multicast group(s) that the interface has joined
MTU	Maximum transmission unit of the interface
ND DAD is enabled, number of DAD attempts	Number of DAD attempts (DAD is enabled). • If DAD is enabled, the number of neighbor request messages is also displayed (configured by using the **ipv6 nd dad attempts** command) • If DAD is disabled, “ND DAD is disabled” is displayed. (You can set the number of neighbor request messages for DAD to 0 to disable this function.)
ND reachable time	Neighbor reachable time
ND retransmit interval	Interval for retransmitting a neighbor solicitation (NS) message
Hosts use stateless autoconfig for addresses	Hosts use stateless autoconfiguration mode to acquire IPv6 addresses
InReceives	All IPv6 packets received by the interface, including all types of error packets.
InTooShorts	Received IPv6 packets that are too short, with a length less than 40 bytes, for example.
InTruncatedPkts	Received IPv6 packets with a length less than that specified in the packets
InHopLimitExceeds	Received IPv6 packets with a hop count exceeding the limit
InBadHeaders	Received IPv6 packets with bad basic headers
InBadOptions	Received IPv6 packets with bad extension headers
ReasmReqds	Received IPv6 fragments
ReasmOKs	Number of packets after reassembly rather than the number of fragments
InFragDrops	IPv6 fragments discarded due to certain error
InFragTimeouts	IPv6 fragments discarded because the interval for which they had stayed in the system buffer exceeded the specified period
OutFragFails	Packets failed in fragmentation on the outbound interface
InUnknownProtos	Received IPv6 packets with unknown or unsupported protocol type
InDelivers	Received IPv6 packets that were delivered to application layer protocols (such as ICMPv6, TCP, and UDP)
OutRequests	Local IPv6 packets sent by IPv6 application protocols
OutForwDatagrams	Packets forwarded by the outbound interface.
InNoRoutes	IPv6 packets that were discarded because no matched route can be found

Field	Description
InTooBigErrors	IPv6 packets that were discarded because they exceeded the PMTU
OutFragOKs	Packets that were fragmented on the outbound interface
OutFragCreates	Number of packet fragments after fragmentation on the outbound interface
InMcastPkts	IPv6 multicast packets received on the interface
InMcastNotMembers	Incoming IPv6 multicast packets that were discarded because the interface did not belong to the corresponding multicast groups
OutMcastPkts	IPv6 multicast packets sent by the interface
InAddrErrors	IPv6 packets that were discarded due to invalid destination addresses
InDiscards	Received IPv6 packets that were discarded due to resource problems rather than packet content errors
OutDiscards	Sent packets that were discarded due to resource problems rather than packet content errors

Display the brief IPv6 information of all interfaces for which IPv6 addresses can be configured.

```
<Sysname> display ipv6 interface
*down: administratively down
(s): spoofing
Interface                         Physical     Protocol     IPv6 Address
Vlan-interface1                   down         down         Unassigned
Vlan-interface2                   up           up           2001::1
Vlan-interface100                 up           down         Unassigned
```

Table 12-6 display ipv6 interface command output description

Field	Description
*down: administratively down	The interface is down, that is, the interface is closed by using the **shutdown** command.
(s): spoofing	Spoofing attribute of the interface, that is, the link protocol state of the interface is up, but the link does not exist, or the link is established on demand, instead of being permanent.
Interface	Name of the interface
Physical	Physical state of the interface: • *down: Indicates that the VLAN interface is administratively down; that is, the interface is shut down using the **shutdown** command. • down: Indicates that the VLAN interface is administratively up but its physical state is down; that is, no port in the VLAN is up, which may be caused by a connection or link failure. • up: Indicates that the administrative and physical states of the VLAN interface are both up.

Field	Description
Protocol	Link protocol state of the interface: • down: Indicates that the link layer protocol state of the VLAN interface is down, generally because no IP address is configured. • up: Indicates that the link layer protocol state of the VLAN interface is up.
IPv6 Address	IPv6 address of the interface. Only the first of configured IPv6 addresses is displayed. (If no address is configured for the interface, “Unassigned” will be displayed.)

display ipv6 neighbors

Syntax

display ipv6 neighbors { { *ipv6-address* | **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-address: IPv6 address whose neighbor information is to be displayed.

all: Displays information of all neighbors, including neighbors acquired dynamically and configured statically.

dynamic: Displays information of all neighbors acquired dynamically.

static: Displays information of all neighbors configured statically.

slot *slot-number*: Displays information of the neighbors of a specified device in an IRF. If no IRF is formed, the neighbors of the current device are displayed only. The *slot-number* argument indicates the member ID of the device.

interface *interface-type interface-number*: Displays information of the neighbors of a specified interface.

vlan *vlan-id*: Displays information of the neighbors of a specified VLAN whose ID ranges from 1 to 4094.

|: Uses a regular expression to match neighbor entries. For detailed information about regular expression, refer to CLI display in *Basic System Configuration* in the *System Volume*.

begin: Displays a specific neighbor entry and all the neighbor entries following it. The specific neighbor entry must match the specified regular expression.

exclude: Displays the neighbor entries not matching the specified regular expression.

include: Displays the neighbor entries matching the specified regular expression.

regular-expression: A case-sensitive string of 1 to 256 characters.

Description

Use the **display ipv6 neighbors** command to display neighbor information.

You can use the **reset ipv6 neighbors** command to clear specific IPv6 neighbor information.

Related commands: **ipv6 neighbor**, **reset ipv6 neighbors**.

Examples

Display all neighbor information.

```
<Sysname> display ipv6 neighbors all
             Type: S-Static    D-Dynamic
IPv6 Address               Link-layer      VID  Interface    State  T   Age
FE80::200:5EFF:FE32:B800   0000-5e32-b800    N/A  GE1/0/1      REACH  S   -
```

Table 12-7 display ipv6 neighbors command output description

Field	Description
IPv6 Address	IPv6 address of a neighbor
Link-layer	Link layer address (MAC address of a neighbor)
VID	VLAN to which the interface connected with a neighbor belongs
Interface	Interface connected with a neighbor
State	State of a neighbor, including: • INCMP: The address is being resolved. The link layer address of the neighbor is unknown. • REACH: The neighbor is reachable. • STALE: The reachability of the neighbor is unknown. The device will not verify the reachability any longer unless data is sent to the neighbor. • DELAY: The reachability of the neighbor is unknown. The device sends an NS message after a delay. • PROBE: The reachability of the neighbor is unknown. The device sends an NS message to verify the reachability of the neighbor.
T	Type of neighbor information, including static configuration and dynamic acquisition.
Age	For a static entry, a hyphen “-“ is displayed. For a dynamic entry, the reachable time (in seconds) elapsed is displayed, and if it is never reachable, “#” is displayed (for a neighbor acquired dynamically).

display ipv6 neighbors count

Syntax

display ipv6 neighbors { { **all** | **dynamic** | **static** } [**slot** *slot-number*] | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count**

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays the total number of all neighbor entries, including neighbor entries acquired dynamically and configured statically.

dynamic: Displays the total number of all neighbor entries acquired dynamically.

static: Displays the total number of neighbor entries configured statically.

slot *slot-number*: Displays the total number of neighbor entries of a specified device in an IRF. If no IRF is formed, the total number of neighbor entries of the current device is displayed only. The *slot-number* argument indicates the member ID of the device.

interface *interface-type interface-number*: Displays the total number of neighbor entries of a specified interface.

vlan *vlan-id*: Displays the total number of neighbor entries of a specified VLAN whose ID ranges from 1 to 4094.

Description

Use the **display ipv6 neighbors count** command to display the total number of neighbor entries satisfying the specified condition.

Examples

Display the total number of neighbor entries acquired dynamically.

```
<Sysname> display ipv6 neighbors dynamic count
Total dynamic entry(ies):  2
```

display ipv6 pathmtu

Syntax

display ipv6 pathmtu { *ipv6-address* | **all** | **dynamic** | **static** }

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-address: IPv6 address whose PMTU information is to be displayed.

all: Displays all PMTU information.

dynamic: Displays all dynamic PMTU information.

static: Displays all static PMTU information.

Description

Use the **display ipv6 pathmtu** command to display the PMTU information of IPv6 addresses.

Examples

Display all PMTU information.

```
<Sysname> display ipv6 pathmtu all
IPv6 Destination Address   ZoneID  PathMTU     Age      Type
 fe80::12                  0       1300        40       Dynamic
 2222::3                   0       1280        -        Static
```

Table 12-8 display ipv6 pathmtu command output description

Field	Description
IPv6 Destination Address	Destination IPv6 address
ZoneID	ID of address zone, currently invalid
PathMTU	PMTU of an IPv6 address
Age	Time for a PMTU to live. For a static PMTU, a hyphen “-“ is displayed.
Type	Indicates that the PMTU is dynamically negotiated or statically configured.

display ipv6 socket

Syntax

display ipv6 socket [**socktype** *socket-type*] [*task-id socket-id*] [**slot** *slot-number*]

View

Any view

Default Level

1: Monitor level

Parameters

socktype *socket-type*: Displays the socket information of this type. The socket type is in the range of 1 to 3. The value “1” represents a TCP socket, “2” a UDP socket, and “3” a raw IP socket.

task-id: Displays the socket information of the task. The task ID is in the range 1 to 100.

socket-id: Displays the information of the socket. The socket ID is in the range 0 to 3072.

slot *slot-number*: Displays the socket information of a specified device in an IRF. If no IRF is formed, the socket information of the current device is displayed only. The *slot-number* argument indicates the member ID of the device.

Description

Use the **display ipv6 socket** command to display socket information.

With no parameter specified, this command displays the information about all the sockets; with only the socket type specified, the command displays the information about sockets of the specified type; with the socket type, task ID and socket ID specified, the command displays the information about the specified socket.

Examples

Display the information of all sockets.

```
<Sysname> display ipv6 socket
```

```
SOCK_STREAM:
Task = VTYD(14), socketid = 4, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC

Task = VTYD(14), socketid = 3, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC

SOCK_DGRAM:
Task = AGNT(51), socketid = 2, Proto = 17,
LA = ::->161, FA = ::->0,
sndbuf = 9216, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEPORT,
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = TRAP(52), socketid = 2, Proto = 17,
LA = ::->1024, FA = ::->0,
sndbuf = 9216, rcvbuf = 42080, sb_cc = 0, rb_cc = 0,
socket option =,
socket state = SS_PRIV

SOCK_RAW:
Task = ROUT(86), socketid = 5, Proto = 89,
LA = ::, FA = ::,
sndbuf = 262144, rcvbuf = 262144, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEADDR,
socket state = SS_PRIV SS_ASYNC
```

Table 12-9 display ipv6 socket command output description

Field	Description
SOCK_STREAM	TCP socket
SOCK_DGRAM	UDP socket
SOCK_RAW	Raw IP socket
Task	Task name and ID of the created socket
socketid	ID assigned by the kernel to the created socket
Proto	Protocol ID
LA	Local address and local port number
FA	Remote address and remote port number
sndbuf	Size of the send buffer
rcvbuf	Size of the receive buffer

Field	Description
sb_cc	Number of bytes sent by the send buffer
rb_cc	Number of bytes received by the receive buffer
socket option	Socket option set by the application
socket state	State of the socket

display ipv6 statistics

Syntax

display ipv6 statistics [**slot** *slot-number*]

View

Any view

Default Level

1: Monitor level

Parameters

slot *slot-number*: Displays statistics of IPv6 packets and ICMPv6 packets on a specified device in an IRF. If no IRF is formed, related information of the current device is displayed only. The *slot-number* argument indicates the member ID of the device.

Description

Use the **display ipv6 statistics** command to display statistics of IPv6 packets and ICMPv6 packets.

You can use the **reset ipv6 statistics** command to clear all IPv6 and ICMPv6 packet statistics.

Examples

Display the statistics of IPv6 packets and ICMPv6 packets.

```
<Sysname> display ipv6 statistics
  IPv6 Protocol:

    Sent packets:
      Total:     0
        Local sent out:     0          forwarded:            0
        raw packets:            0          discarded:        0
        routing failed:     0          fragments:            0
        fragments failed:       0

    Received packets:
      Total:     0
        local host:         0          hopcount exceeded:    0
        format error:           0          option error:     0
        protocol error:     0          fragments:            0
        reassembled:            0          reassembly failed: 0
```

```
    reassembly timeout: 0

ICMPv6 protocol:

  Sent packets:
    Total:     0
      unreached:          0            too big:               0
      hopcount exceeded:  0            reassembly timeout: 0
      parameter problem:  0
      echo request:       0            echo replied:          0
      neighbor solicit:   0            neighbor advert:       0
      router solicit: 0         router advert:     0
      redirected:     0
    Send failed:
      ratelimited:        0            other errors:      0

  Received packets:
    Total:     0
      checksum error: 0           too short:          0
      bad code:           0
      unreached:          0           too big:               0
      hopcount exceeded:  0           reassembly timeout: 0
      parameter problem:  0           unknown error type: 0
      echoed:         0           echo replied:          0
      neighbor solicit:   0           neighbor advert:    0
      router solicit: 0           router advert:         0
      redirected:     0           router renumbering: 0
      unknown info type:  0
    Deliver failed:
      bad length:     0           ratelimited:        0
```

Table 12-10 display ipv6 statistics command output description

Field	Description
IPv6 Protocol:	Statistics of IPv6 packets
Sent packets: Total: 0 Local sent out: 0 forwarded: 0 raw packets: 0 discarded: 0 routing failed: 0 fragments: 0 fragments failed: 0	Statistics of sent IPv6 packets, including: • Total number of locally sent packets and forwarded packets • Number of packets sent locally • Number of forwarded packets • Number of packets sent via raw socket • Number of discarded packets • Number of packets failing to be routed • Number of sent fragment packets • Number of fragments failing to be sent

Field	Description
Received packets: Total: 0 local host: 0 hopcount exceeded: 0 format error: 0 option error: 0 protocol error: 0 fragments: 0 reassembled: 0 reassembly failed: 0 reassembly timeout: 0	Statistics of received IPv6 packets, including • Total number of received packets • Number of packets received locally • Number of packets exceeding the hop limit • Number of packets in an incorrect format • Number of packets with incorrect options • Number of packets with incorrect protocol • Number of received fragment packets • Number of reassembled packets • Number of packets failing to be reassembled • Number of packets whose reassembly times out
ICMPv6 protocol:	Statistics of ICMPv6 packets
Sent packets: Total: 0 unreached: 0 too big: 0 hopcount exceeded: 0 reassembly timeout: 0 parameter problem: 0 echo request: 0 echo replied: 0 neighbor solicit: 0 neighbor advert: 0 router solicit: 0 router advert 0 redirected: 0 Send failed: ratelimited: 0 other errors: 0	Statistics of sent ICMPv6 packets, including • Total number of sent packets • Number of packets whose destination is unreachable • Number of too large packets • Number of packets exceeding the hop limit • Number of packets whose fragmentation and reassembly times out • Number of packets with parameter errors • Number of request packets • Number of response packets • Number of neighbor solicitation packets • Number of neighbor advertisement packets • Number of router solicit packets • Number of router advertisement packets • Number of redirected packets • Number of packets failing to be sent because of rate limitation • Number of packets with other errors

Field	Description
Received packets: Total: 0 checksum error: 0 too short: 0 bad code 0 unreached: 0 too big: 0 hopcount exceeded: 0 reassembly timeout: 0 parameter problem: 0 unknown error type: 0 echoed: 0 echo replied: 0 neighbor solicit: 0 neighbor advert: 0 router solicit: 0 router advert 0 redirected: 0 router renumbering 0 unknown info type: 0 Deliver failed: bad length: 0 ratelimited: 0	Statistics of received ICMPv6 packets, including • Total number of received packets • Number of packets with checksum errors • Number of too small packets • Number of packets with error codes • Number of packets whose destination is unreachable • Number of too large packets • Number of packets exceeding the hop limit • Number of packets whose fragmentation and reassembly times out • Number of packets with parameter errors • Number of packets with unknown errors • Number of request packets • Number of response packets • Number of neighbor solicitation messages • Number of neighbor advertisement packets • Number of router solicitation packets • Number of router advertisement packets • Number of redirected packets • Number of packets recounted by the router • Number of unknown type of packets • Number of packets with a incorrect size • Number of packets failing to be received because of rate limitation

display tcp ipv6 statistics

Syntax

display tcp ipv6 statistics

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display tcp ipv6 statistics** command to display IPv6 TCP connection statistics.

You can use the **reset tcp ipv6 statistics** command to clear statistics of all IPv6 TCP packets.

Examples

Display the statistics of IPv6 TCP connections.

```
<Sysname> display tcp ipv6 statistics
Received packets:
```

```
    Total: 0
    packets in sequence: 0 (0 bytes)
    window probe packets: 0, window update packets: 0
    checksum error: 0, offset error: 0, short error: 0

    duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)
    out-of-order packets: 0 (0 bytes)
    packets with data after window: 0 (0 bytes)
    packets after close: 0

    ACK packets: 0 (0 bytes)
    duplicate ACK packets: 0, too much ACK packets: 0

Sent packets:
    Total: 0
    urgent packets: 0
    control packets: 0 (including 0 RST)
    window probe packets: 0, window update packets: 0

    data packets: 0 (0 bytes) data packets retransmitted: 0 (0 bytes)
    ACK only packets: 0 (0 delayed)

Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 0, keepalive probe: 0, Keepalive timeout, so connections disconnected :
0
Initiated connections: 0, accepted connections: 0, established connections: 0
Closed connections: 0 (dropped: 0, initiated dropped: 0)
```

Table 12-11 display tcp ipv6 statistics command output description

Field	Description
Received packets: Total: 0 packets in sequence: 0 (0 bytes) window probe packets: 0 window update packets: 0 checksum error: 0 offset error: 0 short error: 0 duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes) out-of-order packets: 0 (0 bytes) packets with data after window: 0 (0 bytes) packets after close: 0 ACK packets: 0 (0 bytes) duplicate ACK packets: 0 too much ACK packets: 0	Statistics of received packets, including • Total number of received packets • Number of packets received in sequence • Number of window probe packets • Number of window size update packets • Number of packets with checksum errors • Number of packets with offset errors • Number of packets whose total length is less than specified by the packet header • Number of duplicate packets • Number of partially duplicate packets • Number of out-of-order packets • Number of packets exceeding the size of the receiving window • Number of packets received after the connection is closed • Number of ACK packets • Number of duplicate ACK packets • Number of excessive ACK packets
Sent packets: Total: 0 urgent packets: 0 control packets: 0 (including 0 RST) window probe packets: 0 window update packets: 0 data packets: 0 (0 bytes) data packets retransmitted: 0 (0 bytes) ACK only packets: 0 (0 delayed)	Statistics of sent packets, including • Total number of packets • Number of packets containing an urgent indicator • Number of control packets • Number of window probe packets • Number of window update packets • Number of data packets • Number of retransmitted packets • Number of ACK packets
Retransmitted timeout	Number of packets whose retransmission times out
connections dropped in retransmitted timeout	Number of connections dropped because of retransmission timeout
Keepalive timeout	Number of keepalive timeouts
keepalive probe	Number of keepalive probes
Keepalive timeout, so connections disconnected	Number of connections dropped because of keepalive response timeout
Initiated connections	Number of initiated connections
accepted connections	Number of accepted connections
established connections	Number of established connections
Closed connections	Number of closed connections

Field	Description
dropped	Number of dropped connections (after SYN is received from the peer)
initiated dropped	Number of initiated but dropped connections (before SYN is received from the peer)

display tcp ipv6 status

Syntax

display tcp ipv6 status

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display tcp ipv6** command to display the IPv6 TCP connection status, including IP address of the IPv6 TCP control block, local and peer IPv6 addresses, and status of the IPv6 TCP connection.

Examples

Display the IPv6 TCP connection status.

```
<Sysname> display tcp ipv6 status
TCP6CB      Local Address      Foreign Address     State
045d8074    ::->21              ::->0           Listening
```

Table 12-12 display tcp ipv6 status command output description

Field	Description
TCP6CB	IPv6 address of the TCP control block (hexadecimal)
Local Address	Local IPv6 address
Foreign Address	Remote IPv6 address

Field	Description
State	IPv6 TCP connection status, including • Closed • Listening • Syn_Sent • Syn_Rcvd • Established • Close_Wait • Fin_Wait1 • Closing • Last_Ack • Fin_Wait2 • Time_Wait

display udp ipv6 statistics

Syntax

display udp ipv6 statistics

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display udp ipv6 statistics** command to display the statistics of IPv6 UDP packets.

You can use the **reset udp ipv6 statistics** command to clear the statistics of all IPv6 UDP packets.

Examples

Display the statistics information of IPv6 UDP packets.

```
<Sysname> display udp ipv6 statistics
Received packets:
    Total: 0
    checksum error: 0
    shorter than header: 0, data length larger than packet: 0
    unicast(no socket on port): 0
    broadcast/multicast(no socket on port): 0
    not delivered, input socket full: 0
    input packets missing pcb cache: 0
Sent packets:
    Total: 0
```

Table 12-13 display udp ipv6 statistics command output description

Field	Description
Total	Total number of received/sent packets
checksum error	Total number of packets with a checksum error
shorter than header	Total number of IPv6 UDP packets whose total length is less than that specified by the packet header
data length larger than packet	Total number of packets whose data length exceeds that specified by the packet header
unicast(no socket on port)	Total number of received unicast packets without any socket
broadcast/multicast(no socket on port)	Total number of received broadcast/multicast packets without any socket
not delivered, input socket full	Number of packets not handled because of the receive buffer being full
input packet missing pcb cache	Number of packets failing to match the protocol control block (PCB) cache

dns server ipv6

Syntax

dns server ipv6 *ipv6-address* [*interface-type interface-number*]

undo dns server ipv6 *ipv6-address* [*interface-type interface-number*]

View

System view

Default Level

2: System level

Parameters

ipv6-address: IPv6 address of a DNS server.

interface-type interface-number: Specifies an interface. When the IPv6 address of the DNS server is a link-local address, this argument must be specified.

Description

Use the **dns server ipv6** command to specify a DNS server.

Use the **undo dns server ipv6** command to remove the specified DNS server.

By default, no DNS server is configured.

Examples

Specify a DNS server at 2002::1.

```
<Sysname> system-view
[Sysname] dns server ipv6 2002::1
```

ipv6

Syntax

ipv6

undo ipv6

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **ipv6** command to enable IPv6.

Use the **undo ipv6** command to disable IPv6.

By default, IPv6 is disabled.

Examples

Enable IPv6.

```
<Sysname> system-view
[Sysname] ipv6
```

ipv6 address

Syntax

ipv6 address { *ipv6-address prefix-length* | *ipv6-address***/***prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address***/***prefix-length*]

View

Interface view

Default Level

2: System level

Parameters

ipv6-address: IPv6 address.

prefix-length: Prefix length of the IPv6 address, in the range 1 to 128.

Description

Use the **ipv6 address** command to configure an IPv6 site-local address or aggregatable global unicast address for an interface.

Use the **undo ipv6 address** command to remove the IPv6 address from the interface.

By default, no site-local address or global unicast address is configured for an interface.

Note that except the link-local address automatically configured, all IPv6 addresses will be removed from the interface if you carry out the **undo ipv6 address** command without any parameter specified.

Examples

Set the aggregatable global IPv6 unicast address of VLAN-interface 100 to 2001::1 with prefix length 64.

Method I:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64
```

Method II:

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1 64
```

ipv6 address auto link-local

Syntax

ipv6 address auto link-local

undo ipv6 address auto link-local

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **ipv6 address auto link-local** command to automatically generate a link-local address for an interface.

Use the **undo ipv6 address auto link-local** command to remove the automatically generated link-local address for the interface.

By default, a link-local address will automatically be generated after a site-local or global IPv6 unicast address is configured for an interface.

Note that:

- After an IPv6 site-local address or aggregatable global unicast address is configured for an interface, a link-local address is generated automatically. The automatically generated link-local address is the same as the one generated by using the **ipv6 address auto link-local** command.
- The **undo ipv6 address auto link-local** command can only remove the link-local addresses generated through the **ipv6 address auto link-local** command. Therefore, after the **undo ipv6 address auto link-local** command is used on an interface that has an IPv6 site-local address or

aggregatable global unicast address configured, the interface still has a link-local address. If the interface has no IPv6 site-local address or aggregatable global unicast address configured, it will have no link-local address.

- Manual assignment takes precedence over automatic generation. That is, if you first adopt automatic generation and then manual assignment, the manually assigned link-local address will overwrite the automatically generated one. If you first adopt manual assignment and then automatic generation, the automatically generated link-local address will not take effect and the link-local address of an interface is still the manually assigned one. If you delete the manually assigned address, the automatically generated link-local address is validated. For manually assignment of an IPv6 link-local address, refer to the **ipv6 address link-local** command.

Examples

Configure VLAN-interface 100 to automatically generate a link-local address.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address auto link-local
```

ipv6 address eui-64

Syntax

ipv6 address *ipv6-addressIprefix-length* **eui-64**

undo ipv6 address *ipv6-addressIprefix-length* **eui-64**

View

Interface view

Default Level

2: System level

Parameters

ipv6-addressIprefix-length: IPv6 address and IPv6 prefix. The *ipv6-address* and *prefix-length* arguments jointly specify the prefix of an IPv6 address in the EUI-64 format.

Description

Use the **ipv6 address eui-64** command to configure a site-local address or global unicast address in the EUI-64 format for an interface.

Use the **undo ipv6 address eui-64** command to remove the configured site-local address or global unicast address in the EUI-64 format for the interface.

By default, no site-local or global unicast address in the EUI-64 format is configured for an interface.

An EUI-64 IPv6 address is generated based on the specified prefix and the MAC address of the local device and can be displayed by using the **display ipv6 interface** command.

Note that you cannot specify the prefix length of an IPv6 address in the EUI-64 format to be greater than 64.

Examples

Configure an IPv6 address in the EUI-64 format for VLAN-interface 100. The prefix length of the address is the same as that of 2001::1/64, and the interface ID is generated based on the MAC address of the device.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address 2001::1/64 eui-64
```

ipv6 address link-local

Syntax

ipv6 address *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

View

Interface view

Default Level

2: System level

Parameters

ipv6-address: IPv6 link-local address. The first 10 bits of an address must be 1111111010 (binary), that is, the first group of hexadecimals in the address must be FE80 to FEBF.

Description

Use the **ipv6 address link-local** command to configure a link-local address for the interface.

Use the **undo ipv6 address link-local** command to remove the configured link-local address for the interface.

Note that:

Manual assignment takes precedence over automatic generation. That is, if you first adopt automatic generation and then manual assignment, the manually assigned link-local address will overwrite the automatically generated one. If you first adopt manual assignment and then automatic generation, the automatically generated link-local address will not take effect and the link-local address of an interface is still the manually assigned one. If you delete the manually assigned address, the automatically generated link-local address is validated. For automatic generation of an IPv6 link-local address, refer to the **ipv6 address auto link-local** command.

Examples

Configure a link-local address for VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 address fe80::1 link-local
```

ipv6 hoplimit-expires enable

Syntax

ipv6 hoplimit-expires enable

undo ipv6 hoplimit-expires

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **ipv6 hoplimit-expires enable** command to enable the sending of ICMPv6 time exceeded packets.

Use the **undo ipv6 hoplimit-expires** command to disable the sending of ICMPv6 time exceeded packets.

By default, the sending of ICMPv6 time exceeded packets is enabled.

Note that:

After you disable the sending of ICMPv6 time exceeded packets, the device will not send time-to-live count exceeded packets, but will still send fragment reassembly time exceeded packets.

Examples

Disable the sending of ICMPv6 time exceeded packets.

```
<Sysname> system-view
[Sysname] undo ipv6 hoplimit-expires
```

ipv6 host

Syntax

ipv6 host *hostname ipv6-address*

undo ipv6 host *hostname* [*ipv6-address*]

View

System view

Default Level

2: System level

Parameters

hostname: Host name, a string of up to 20 characters. The character string can contain letters, numerals, “_”, “-“, or “.” and must contain at least one letter.

ipv6-address: IPv6 address.

Description

Use the **ipv6 host** command to configure the mappings between host names and IPv6 addresses.

Use the **undo ipv6 host** command to remove the mappings between host names and IPv6 addresses.

Each host name can correspond to only one IPv6 address.

Related commands: **display ipv6 host**.

Examples

Configure the mapping between a host name and an IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 host aaa 2001::1
```

ipv6 icmp-error

Syntax

ipv6 icmp-error { **bucket** *bucket-size* | **ratelimit** *interval* } *

undo ipv6 icmp-error

View

System view

Default Level

2: System level

Parameters

bucket *bucket-size*: Number of tokens in the token bucket, in the range of 1 to 200.

ratelimit *interval*: Update period of the token bucket in milliseconds, in the range of 0 to 2,147,483,647. The update period “0” indicates that the number of ICMPv6 error packets sent is not restricted.

Description

Use the **ipv6 icmp-error** command to configure the size and update period of the token bucket.

Use the **undo ipv6 icmp-error** command to restore the defaults.

By default, the size is 10 and the update period is 100 milliseconds. That is, at most 10 ICMPv6 error packets can be sent within 100 milliseconds.

Examples

Set the capacity of the token bucket to 50 and the update period to 100 milliseconds.

```
<Sysname> system-view
[Sysname] ipv6 icmp-error bucket 50 ratelimit 100
```

ipv6 icmpv6 multicast-echo-reply enable

Syntax

ipv6 icmpv6 multicast-echo-reply enable

undo ipv6 icmpv6 multicast-echo-reply

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **ipv6 icmpv6 multicast-echo-reply enable** command to enable the sending of multicast echo replies.

Use the **undo ipv6 icmpv6 multicast-echo-reply** command to disable the sending of multicast echo replies.

By default, the device is disabled from sending multicast echo replies.

Examples

Enable the sending of multicast echo replies.

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 multicast-echo-reply enable
```

ipv6 nd autoconfig managed-address-flag

Syntax

ipv6 nd autoconfig managed-address-flag

undo ipv6 nd autoconfig managed-address-flag

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **ipv6 nd autoconfig managed-address-flag** command to set the managed address configuration (M) flag to 1 so that the host can acquire an IPv6 address through stateful autoconfiguration (for example, from a DHCP server).

Use the **undo ipv6 nd autoconfig managed-address-flag** command to restore the default.

By default, the M flag is set to **0** so that the host can acquire an IPv6 address through stateless autoconfiguration.

Examples

Configure the host to acquire an IPv6 address through stateful autoconfiguration.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

ipv6 nd autoconfig other-flag

Syntax

ipv6 nd autoconfig other-flag

undo ipv6 nd autoconfig other-flag

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **ipv6 nd autoconfig other-flag** command to set the other stateful configuration flag (O) to 1 so that the host can acquire information other than IPv6 address through stateful autoconfiguration (for example, from a DHCP server).

Use the **undo ipv6 nd autoconfig other-flag** command to restore the default.

By default, the O flag is set to **0** so that the host can acquire other information through stateless autoconfiguration.

Examples

Configure the host to acquire information other than IPv6 address through stateless autoconfiguration.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] undo ipv6 nd autoconfig other-flag
```

ipv6 nd dad attempts

Syntax

ipv6 nd dad attempts *value*

undo ipv6 nd dad attempts

View

Interface view

Default Level

2: System level

Parameters

value: Number of attempts to send an NS message for DAD, in the range of 0 to 600. The default value is “1”. When it is set to 0, DAD is disabled.

Description

Use the **ipv6 nd dad attempts** command to configure the number of attempts to send an NS message for DAD.

Use the **undo ipv6 nd dad attempts** command to restore the default.

By default, the number of attempts to send an NS message for DAD is 1.

Related commands: **display ipv6 interface**.

Examples

Set the number of attempts to send an NS message for DAD to 20.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd dad attempts 20
```

ipv6 nd hop-limit

Syntax

ipv6 nd hop-limit *value*

undo ipv6 nd hop-limit

View

System view

Default Level

2: System level

Parameters

value: Number of hops, in the range of 0 to 255. When it is set to 0, the Hop Limit field in RA messages sent by the device is 0. That is, the number of hops is determined by the requesting device itself.

Description

Use the **ipv6 nd hop-limit** command to configure the hop limit advertised by the device.

Use the **undo ipv6 nd hop-limit** command to restore the default hop limit.

By default, the hop limit advertised by the device is 64.

Examples

Set the hop limit advertised by the device to 100.

```
<Sysname> system-view
[Sysname] ipv6 nd hop-limit 100
```

ipv6 nd ns retrans-timer

Syntax

ipv6 nd ns retrans-timer *value*

undo ipv6 nd ns retrans-timer

View

Interface view

Default Level

2: System level

Parameters

value: Interval for retransmitting an NS message in milliseconds, in the range of 1,000 to 4,294,967,295.

Description

Use the **ipv6 nd ns retrans-timer** command to set the interval for retransmitting an NS message. The local interface retransmits an NS message at intervals of this value. Furthermore, the Retrans Timer field in RA messages sent by the local interface is equal to this value.

Use the **undo ipv6 nd ns retrans-timer** command to restore the default.

By default, the local interface retransmits an NS message at intervals of 1,000 milliseconds and the Retrans Timer field in RA messages sent by the local interface is 0.

Related commands: **display ipv6 interface**.

Examples

Specify VLAN-interface 100 to retransmit NS messages at intervals of 10,000 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ns retrans-timer 10000
```

ipv6 nd nud reachable-time

Syntax

ipv6 nd nud reachable-time *value*

undo ipv6 nd nud reachable-time

View

Interface view

Default Level

2: System level

Parameters

value: Neighbor reachable time in milliseconds, in the range of 1 to 3,600,000.

Description

Use the **ipv6 nd nud reachable-time** command to configure the neighbor reachable time on an interface. This time value serves as not only the neighbor reachable time on the local interface, but also the value of the Reachable Timer field in RA messages sent by the local interface.

Use the **undo ipv6 nd nud reachable-time** command to restore the default neighbor reachable time and to specify the value of the Reachable Timer field in RA messages as 0, so that the number of hops is determined by the requesting device itself.

By default, the neighbor reachable time on the local interface is 30,000 milliseconds and the Reachable Timer field in RA messages is 0.

Related commands: **display ipv6 interface**.

Examples

Set the neighbor reachable time on VLAN-interface 100 to 10,000 milliseconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd nud reachable-time 10000
```

ipv6 nd ra halt

Syntax

ipv6 nd ra halt

undo ipv6 nd ra halt

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **ipv6 nd ra halt** command to enable RA message suppression.

Use the **undo ipv6 nd ra halt** command to disable RA message suppression.

By default, RA messages are suppressed.

Examples

Suppress RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra halt
```

ipv6 nd ra interval

Syntax

ipv6 nd ra interval *max-interval-value min-interval-value*

undo ipv6 nd ra interval

View

Interface view

Default Level

2: System level

Parameters

max-interval-value: Maximum interval for advertising RA messages in seconds, in the range of 4 to 1,800.

min-interval-value: Minimum interval for advertising RA messages in seconds, in the range of 3 to 1,350.

Description

Use the **ipv6 nd ra interval** command to set the maximum and minimum intervals for advertising RA messages. The device advertises RA messages at intervals of a random value between the maximum interval and the minimum interval.

Use the **undo ipv6 nd ra interval** command to restore the default.

By default, the maximum interval between RA messages is 600 seconds, and the minimum interval is 200 seconds.

Note the following:

- The minimum interval should be three-fourths of the maximum interval or less.
- The maximum interval for sending RA messages should be less than or equal to the router lifetime in RA messages.

Examples

Set the maximum interval for advertising RA messages to 1,000 seconds and the minimum interval to 700 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra interval 1000 700
```

ipv6 nd ra prefix

Syntax

ipv6 nd ra prefix { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } *valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] *

undo ipv6 nd ra prefix *ipv6-prefix*

View

Interface view

Default Level

2: System level

Parameters

ipv6-address: IPv6 address or IPv6 address prefix.

prefix-length: Prefix length of the IPv6 address.

ipv6-prefix: IPv6 address prefix.

valid-lifetime: Valid lifetime of a prefix in seconds, in the range of 0 to 4,294,967,295.

preferred-lifetime: Preferred lifetime of a prefix used for stateless autoconfiguration in seconds, in the range of 0 to 4,294,967,295.

no-autoconfig: Specifies a prefix not to be used for stateless autoconfiguration. If this keyword is not provided, the prefix is used for stateless autoconfiguration.

off-link: Specifies the address with the prefix not to be directly reachable on the link. If this keyword is not provided, the address with the prefix is directly reachable on the link.

Description

Use the **ipv6 nd ra prefix** command to configure the prefix information in RA messages.

Use the **undo ipv6 nd ra prefix** command to remove the prefix information from RA messages.

By default, no prefix information is configured in RA messages and the IPv6 address of the interface sending RA messages is used as the prefix information.

Examples

Configure the prefix information for RA messages on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra prefix 2001:10::100/64 100 10
```

ipv6 nd ra router-lifetime

Syntax

ipv6 nd ra router-lifetime *value*

undo ipv6 nd ra router-lifetime

View

Interface view

Default Level

2: System level

Parameters

value: Router lifetime in seconds, in the range of 0 to 9,000. When it is set to 0, the device does not serve as the default router.

Description

Use the **ipv6 nd ra router-lifetime** command to configure the router lifetime in RA messages.

Use the **undo ipv6 nd ra router-lifetime** command to restore the default.

By default, the router lifetime in RA messages is 1,800 seconds.

Note that the router lifetime in RA messages should be greater than or equal to the advertising interval.

Examples

Set the router lifetime in RA messages on VLAN-interface 100 to 1,000 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra router-lifetime 1000
```

ipv6 neighbor

Syntax

ipv6 neighbor *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* }

undo ipv6 neighbor *ipv6-address interface-type interface-number*

View

System view

Default Level

2: System level

Parameters

ipv6-address: IPv6 address of the static neighbor entry.

mac-address: MAC address of the static neighbor entry (48 bits long, in the format of H-H-H).

vlan-id: VLAN ID of the static neighbor entry, in the range of 1 to 4094.

port-type port-number: Type and number of a Layer 2 port of the static neighbor entry.

interface *interface-type interface-number*: Type and number of a Layer 3 interface of the static neighbor entry.

Description

Use the **ipv6 neighbor** command to configure a static neighbor entry.

Use the **undo ipv6 neighbor** command to remove a static neighbor entry.

You can use a Layer 3 VLAN interface or a Layer 2 port in the VLAN to configure a static neighbor entry.

- If the first method is used, the neighbor entry is in the INCMP state. After the device obtains the corresponding Layer 2 port information through resolution, the neighbor entry will go into the REACH state.
- If the second method is used, the corresponding VLAN interface must exist and the port specified by *port-type port-number* must belong to the VLAN specified by *vlan-id*. After the static neighbor entry is configured, the device will relate the VLAN interface with the IPv6 address to identify the static neighbor entry uniquely and the entry will be in the REACH state.

To remove a static neighbor entry, you only need to specify the corresponding VLAN interface and the neighbor address.

Related commands: **display ipv6 neighbors**.

Examples

Configure a static neighbor entry for Layer 2 port GigabitEthernet1/0/1 of VLAN 100.

```
<Sysname> system-view
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 100 gigabitethernet 1/0/1
```

ipv6 neighbors max-learning-num

Syntax

ipv6 neighbors max-learning-num *number*

undo ipv6 neighbors max-learning-num

View

Interface view

Default Level

2: System level

Parameters

number: Maximum number of neighbors that can be dynamically learned by the interface, in the range 1 to 128.

Description

Use the **ipv6 neighbors max-learning-num** command to configure the maximum number of neighbors that can be dynamically learned on the interface.

Use the **undo ipv6 neighbors max-learning-num** command to restore the default.

By default, the maximum number of neighbors that can be dynamically learned on the interface is 128.

Examples

Set the maximum number of neighbors that can be dynamically learned on VLAN-interface 100 to 10.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 neighbors max-learning-num 10
```

ipv6 pathmtu

Syntax

ipv6 pathmtu *ipv6-address* [*value*]

undo ipv6 pathmtu *ipv6-address*

View

System view

Default Level

2: System level

Parameters

ipv6-address: IPv6 address.

value: PMTU of a specified IPv6 address in bytes. It ranges from 1280 to 10000.

Description

Use the **ipv6 pathmtu** command to configure a static PMTU for a specified IPv6 address.

Use the **undo ipv6 pathmtu** command to remove the PMTU configuration for a specified IPv6 address.

By default, no static PMTU is configured.

Examples

Configure a static PMTU for a specified IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu fe80::12 1300
```

ipv6 pathmtu age

Syntax

ipv6 pathmtu age *age-time*

undo ipv6 pathmtu age

View

System view

Default Level

2: System level

Parameters

age-time: Aging time for PMTU in minutes, in the range of 10 to 100.

Description

Use the **ipv6 pathmtu age** command to configure the aging time for a dynamic PMTU.

Use the **undo ipv6 pathmtu age** command to restore the default.

By default, the aging time is 10 minutes.

Note that the aging time is invalid for a static PMTU.

Related commands: **display ipv6 pathmtu**.

Examples

Set the aging time for a dynamic PMTU to 40 minutes.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu age 40
```

reset dns ipv6 dynamic-host

Syntax

reset dns ipv6 dynamic-host

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **reset dns ipv6 dynamic-host** command to clear IPv6 dynamic domain name cache information.

You can use the **display dns ipv6 dynamic-host** command to display the current IPv6 dynamic domain name cache information.

Examples

Clear IPv6 dynamic domain name cache information.

```
<Sysname> reset dns ipv6 dynamic-host
```

reset ipv6 neighbors

Syntax

reset ipv6 neighbors { **all** | **dynamic** | **interface** *interface-type interface-number* | **slot** *slot-number* | **static** }

View

User view

Default Level

2: System level

Parameters

all: Clears static and dynamic neighbor information on all interfaces.

dynamic: Clears dynamic neighbor information on all interfaces.

interface *interface-type interface-number*: Clears dynamic neighbor information on a specified interface.

slot *slot-number*: Clears dynamic neighbor information on a specified device in an IRF. If no IRF is formed, only the dynamic neighbor information of the current device is cleared. The *slot-number* argument indicates the member ID of the device.

static: Clears static neighbor information on all interfaces.

Description

Use the **reset ipv6 neighbors** command to clear IPv6 neighbor information.

You can use the **display ipv6 neighbors** command to display the current IPv6 neighbor information.

Examples

Clear neighbor information on all interfaces.

```
<Sysname> reset ipv6 neighbors all
```

Clear dynamic neighbor information on all interfaces.

```
<Sysname> reset ipv6 neighbors dynamic
```

Clear all neighbor information on VLAN-interface 1.

```
<Sysname> reset ipv6 neighbors interface vlan-interface 1
```

reset ipv6 pathmtu

Syntax

reset ipv6 pathmtu { **all** | **static** | **dynamic** }

View

User view

Default Level

2: System level

Parameters

all: Clears all PMTUs.

static: Clears all static PMTUs.

dynamic: Clears all dynamic PMTUs.

Description

Use the **reset ipv6 pathmtu** the command to clear the PMTU information.

Examples

Clear all PMTUs.

```
<Sysname> reset ipv6 pathmtu all
```

reset ipv6 statistics

Syntax

reset ipv6 statistics [**slot** *slot-number*]

View

User view

Default Level

2: System level

Parameters

slot *slot number*: Clears the statistics of IPv6 packets and ICMPv6 packets on a specified device in an IRF. If no IRF is formed, related information on the current device is cleared only. The *slot-number* argument indicates the member ID of the device.

Description

Use the **reset ipv6 statistics** command to clear the statistics of IPv6 packets and ICMPv6 packets.

You can use the **display ipv6 statistics** command to display the statistics of IPv6 and ICMPv6 packets.

Examples

Clear the statistics of IPv6 packets and ICMPv6 packets.

```
<Sysname> reset ipv6 statistics
```

reset tcp ipv6 statistics

Syntax

reset tcp ipv6 statistics

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **reset tcp ipv6 statistics** command to clear the statistics of all IPv6 TCP connections.

You can use the **display tcp ipv6 statistics** command to display the statistics of IPv6 TCP connections.

Examples

Clear the statistics of all IPv6 TCP connections.

```
<Sysname> reset tcp ipv6 statistics
```

reset udp ipv6 statistics

Syntax

reset udp ipv6 statistics

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **reset udp ipv6 statistics** command to clear the statistics of all IPv6 UDP packets.

You can use the **display udp ipv6 statistics** command to display the statistics of IPv6 UDP packets.

Examples

Clear the statistics of all IPv6 UDP packets.

```
<Sysname> reset udp ipv6 statistics
```

tcp ipv6 timer fin-timeout

Syntax

tcp ipv6 timer fin-timeout *wait-time*

undo tcp ipv6 timer fin-timeout

View

System view

Default Level

2: System level

Parameters

wait-time: Length of the finwait timer for IPv6 TCP connections in seconds, in the range of 76 to 3,600.

Description

Use the **tcp ipv6 timer fin-timeout** command to set the finwait timer for IPv6 TCP connections.

Use the **undo tcp ipv6 timer fin-timeout** command to restore the default.

By default, the length of the finwait timer is 675 seconds.

Examples

Set the finwait timer length of IPv6 TCP connections to 800 seconds.

```
<Sysname> system-view
[Sysname] tcp ipv6 timer fin-timeout 800
```

tcp ipv6 timer syn-timeout

Syntax

tcp ipv6 timer syn-timeout *wait-time*

undo tcp ipv6 timer syn-timeout

View

System view

Default Level

2: System level

Parameters

wait-time: Length of the synwait timer for IPv6 TCP connections in seconds, in the range of 2 to 600.

Description

Use the **tcp ipv6 timer syn-timeout** command to set the synwait timer for IPv6 TCP connections

Use the **undo tcp ipv6 timer syn-timeout** command to restore the default.

By default, the length of the synwait timer of IPv6 TCP connections is 75 seconds.

Examples

Set the synwait timer length of IPv6 TCP connections to 100 seconds.

```
<Sysname> system-view
[Sysname] tcp ipv6 timer syn-timeout 100
```

tcp ipv6 window

Syntax

tcp ipv6 window *size*

undo tcp ipv6 window

View

System view

Default Level

2: System level

Parameters

size: Size of the IPv6 TCP send/receive buffer in KB (kilobyte), in the range of 1 to 32.

Description

Use the **tcp ipv6 window** command to set the size of the IPv6 TCP send/receive buffer.

Use the **undo tcp ipv6 window** command to restore the default.

By default, the size of the IPv6 TCP send/receive buffer is 8 KB.

Examples

Set the size of the IPv6 TCP send/receive buffer to 4 KB.

```
<Sysname> system-view
[Sysname] tcp ipv6 window 4
```

13 sFlow Configuration Commands

sFlow Configuration Commands

display sflow

Syntax

display sflow [**slot** *slot-number*]

View

Any view

Default Level

2: System level

Parameters

slot *slot-number*: Displays the sFlow configuration information of the specified IRF member device. The *slot-number* argument is the member number of the device in the IRF, which you can display with the **display irf** command. The value range for the *slot-number* argument depends on the number of members and numbering conditions in the current IRF. If no IRF exists, the *slot-number* argument is the current device number.

Description

Use the **display sflow** command to display the sFlow configuration information.

Examples

Display the sFlow configuration information of member device 1 in an IRF stack.

```
<Sysname> display sflow slot 1
sFlow Version: 5
sFlow Global Information:
   Agent       IP:10.10.10.1
   Collector   IP:10.10.10.2  Port:6343
   Interval(s): 20
sFlow Port Information:
Interface                Direction       Rate         Mode          Status
GigabitEthernet1/0/1     Out             5000         Random        Active
```

Table 13-1 display sflow command output description

Field	Description
sFlow Version	Currently, sFlow has the following versions: • 4: sFlow version 4. • 5: sFlow version 5.

Field	Description
sFlow Global Information	sFlow global configuration information
Agent	IP address of the sFlow agent
Collector	IP address and port number of each sFlow collector
Interval(s)	Counter sampling interval (sFlow interval)
sFlow Port Information	Information of the ports enabled with sFlow
Interface	sFlow enabled interface
Direction	Packet sampling direction: • In: Samples inbound packets. • Out: Samples outbound packets. • In/Out: Samples inbound and outbound packets.
Rate	Packet sampling rate
Mode	Packet sampling mode: • Determine: Samples a fixed number of packets. • Random: Samples a random number of packets.
Status	Status of the sFlow enabled port: • Suspend: Indicates the port is suspended, and it stops sampling. • Active: Indicates the port is active and performs sampling.

sflow agent ip

Syntax

sflow agent ip *ip-address*

undo sflow agent ip

View

System view

Default Level

2: System level

Parameters

ip-address: IP address of the sFlow agent.

Description

Use the **sflow agent ip** command to configure the IP address of the sFlow agent.

Use the **undo sflow agent ip** command to remove the configured IP address.

By default, no IP address is configured for the sFlow agent.

Note that:

- The sFlow agent and sFlow collector must not have the same IP address.
- Currently, a device supports only one sFlow agent.

- sFlow does not work if the sFlow agent has no IP address configured, or the IP address of the sFlow agent is removed.

Examples

Configure the IP address of the sFlow agent.

```
<Sysname> system-view
[Sysname] sflow agent ip 10.10.10.1
```

sflow collector ip

Syntax

sflow collector ip *ip-address* [**port** *portnum*]

undo sflow collector ip *ip-address*

View

System view

Default Level

2: System level

Parameters

ip-address: IP address of the sFlow collector.

port *portnum*: Port number of the sFlow Collector, which is in the range 1 to 65535 and defaults to 6343.

Description

Use the **sflow collector ip** command to specify the IP address and port number of an sFlow collector.

Use the **undo sflow collector ip** command to remove an sFlow collector.

By default, no sFlow collector is specified.

Note that:

- The sFlow collector and sFlow agent must not have the same IP address.
- Currently, you can specify at most two sFlow collectors, with one as the backup sFlow collector.
- sFlow does not work if no sFlow collector is specified.
- If only one sFlow collector is specified, sFlow does not work after you use the **undo sflow collector ip** command to disable it.

Examples

Specify the IP address and port number of an sFlow collector.

```
<Sysname> system-view
[Sysname] sflow collector ip 10.10.10.2 port 6343
```

sflow enable

Syntax

sflow enable { **inbound** | **outbound** }

undo sflow enable { **inbound** | **outbound** }

View

Ethernet port view

Default Level

2: System level

Parameters

inbound: Samples inbound packets.

outbound: Samples outbound packets.

Description

Use the **sflow enable** command to enable sFlow in the inbound or outbound direction on the port.

Use the **undo sflow enable** command to disable sFlow in the inbound or outbound direction on the port.

sFlow is disabled by default.

Note that:

This command is supported on physical Ethernet interfaces only, instead of logical interfaces (VLAN interfaces). If you want to enable sFlow on an aggregation group, you need to enable sFlow on each member port.

Examples

Enable sFlow in the outbound direction on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sflow enable outbound
```

sflow interval

Syntax

sflow interval *interval-time*

undo sflow interval

View

System view

Default Level

2: System level

Parameters

interval-time: Counter sampling interval in seconds, in the range 2 to 200.

Description

Use the **sflow interval** command to set the counter sampling interval at which the sFlow agent collects the statistics of all sFlow enabled ports.

Use the **undo sflow interval** command to restore the default interval.

By default, the sampling interval is 20 seconds.

Examples

Configure the counter sampling interval as 50 seconds.

```
<Sysname> system-view
[Sysname] sflow interval 50
```

sflow sampling-mode

Syntax

sflow sampling-mode { **determine** | **random** }

undo sflow sampling-mode

View

Ethernet port view

Default Level

2: System level

Parameters

determine: Sample a fixed number of packets.

random: Sample packets randomly.

Description

Use the **sflow sampling-mode** command to specify the packet sampling mode.

Use the **undo sflow sampling-mode** command to restore the default.

By default, the packet sampling mode is **random**.

Note that this command should be used after sFlow is enabled on the current port.

Note

Currently, the **determine** mode is not supported on Switch 4210G Family.

Examples

Configure the interface to sample a fixed number of inbound packets.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sflow enable inbound
[Sysname-GigabitEthernet1/0/1] sflow sampling-mode determine
```

sflow sampling-rate

Syntax

sflow sampling-rate *rate*

undo sflow sampling-rate

View

Ethernet port view

Default Level

2: System level

Parameters

rate: Number of packets, in the range of 1000 to 500000.

Description

Use the **sflow sampling-rate** command to specify the number of packets out of which the interface will sample a packet.

Use the **undo sflow sampling-rate** command to restore the default.

By default, the packet sampling rate is 200000.

Note that this command should be used after sFlow is enabled on the current port.

Examples

Specify the interface to sample a packet out of 100000 inbound packets.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] sflow enable inbound
[Sysname-GigabitEthernet1/0/1] sflow sampling-rate 100000
```

Table of Contents

1 IP Routing Table Commands

Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

IP Routing Table Commands

display ip routing-table

Syntax

display ip routing-table [**verbose** | | { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

verbose: Displays detailed routing table information, including that for inactive routes. With this keyword absent, the command displays only brief information about active routes.

|: Uses a regular expression to filter output information. For details about regular expressions, refer to the section *CLI Display* in *Basic System Configuration* in the *System Volume*.

begin: Displays route entries starting from the one specified by the regular expression.

exclude: Displays route entries not matching the regular expression.

include: Displays route entries matching the regular expression.

regular-expression: Regular expression, a string of 1 to 256 case-sensitive characters used for specifying routing entries.

Description

Use the **display ip routing-table** command to display brief information about active routes in the routing table.

This command displays brief information about a routing table, with a routing entry contained in one line. The information displayed includes destination IP address/mask length, protocol, priority, cost, next hop and outbound interface. This command only displays the routes currently in use, that is, the optimal routes.

Use the **display ip routing-table verbose** command to display detailed information about all routes in the routing table.

This command displays detailed information about all active and inactive routes, including the statistics of the entire routing table and information for each route.

Examples

Display brief information about active routes in the routing table.

```
<Sysname> display ip routing-table
Routing Tables: Public
        Destinations : 4        Routes : 4
Destination/Mask    Proto  Pre  Cost        NextHop         Interface
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
192.168.80.0/24     Direct 0    0           192.168.80.10   Vlan1
192.168.80.10/32    Direct 0    0           127.0.0.1       InLoop0
```

Table 1-1 display ip routing-table command output description

Field	Description
Destinations	Number of destination addresses
Routes	Number of routes
Destination/Mask	Destination address/mask length
Proto	Protocol that presents the route
Pre	Priority of the route
Cost	Cost of the route
Nexthop	Address of the next hop on the route
Interface	Outbound interface for packets to be forwarded along the route

Display detailed information about all routes in the routing table.

```
<Sysname> display ip routing-table verbose
Routing Table : Public
        Destinations : 4        Routes : 4

  Destination: 10.1.1.0/24
     Protocol: Direct         Process ID: 0
   Preference: 0                  Cost: 0
      NextHop: 10.1.1.1        Interface: Vlan-interface1
  RelyNextHop: 0.0.0.0         Neighbour: 0.0.0.0
    Tunnel ID: 0x0                Label: NULL
        State: Active Adv           Age: 04h00m30s
          Tag: 0
  Destination: 10.1.1.1/32
     Protocol: Direct         Process ID: 0
   Preference: 0                  Cost: 0
      NextHop: 127.0.0.1       Interface: InLoopBack0
```

```
RelyNextHop: 0.0.0.0        Neighbour: 0.0.0.0
  Tunnel ID: 0x0              Label: NULL
      State: Active NoAdv       Age: 04h00m30s
        Tag: 0

Destination: 127.0.0.0/8
   Protocol: Direct        Process ID: 0
 Preference: 0                Cost: 0
    NextHop: 127.0.0.1      Interface: InLoopBack0
RelyNextHop: 0.0.0.0        Neighbour: 0.0.0.0
  Tunnel ID: 0x0              Label: NULL
      State: Active NoAdv       Age: 04h00m36s
        Tag: 0

Destination: 127.0.0.1/32
   Protocol: Direct        Process ID: 0
 Preference: 0                Cost: 0
    NextHop: 127.0.0.1      Interface: InLoopBack0
RelyNextHop: 0.0.0.0        Neighbour: 0.0.0.0
  Tunnel ID: 0x0              Label: NULL
      State: Active NoAdv       Age: 04h00m36s
        Tag: 0
```

Displayed first are statistics for the whole routing table, followed by detailed description of each route (in sequence).

Table 1-2 display ip routing-table verbose command output description

Field	Description
Destination	Destination address/mask length
Protocol	Protocol that presents the route
Process ID	Process ID
Preference	Priority of the route
Cost	Cost of the route
NextHop	Address of the next hop on the route
Interface	Outbound interface for packets to be forwarded along the route
BkNexthop	Backup next hop
BkInterface	Backup outbound interface
RelyNextHop	The next hop address obtained through routing recursion
Neighbour	Neighboring address determined by Routing Protocol
Tunnel ID	Tunnel ID
Label	Label

Field	Description	
State	Route status:	
	Active	This is an active unicast route.
	Adv	This route can be advertised.
	Delete	This route is deleted.
	Gateway	This is an indirect route.
	Holddown	Number of holddown routes.
	Int	The route was discovered by an Interior Gateway Protocol (IGP).
	NoAdv	The route is not advertised when the router advertises routes based on policies.
	NotInstall	Normally, among routes to a destination, the route with the highest priority is installed into the core routing table and advertised, while a NotInstall route cannot be installed into the core routing table but may be advertised.
	Reject	The packets matching a Reject route will be dropped. Besides, the router sends ICMP unreachable messages to the sources of the dropped packets. The Reject routes are usually used for network testing.
	Static	A static route is not lost when you perform the save operation and then restart the router. Routes configured manually are marked as **static**.
	Unicast	Unicast routes
	Inactive	Inactive routes
	Invalid	Invalid routes
	WaitQ	The route is the WaitQ during route recursion.
	TunE	Tunnel
	GotQ	The route is in the GotQ during route recursion.
Age	Time for which the route has been in the routing table, in the sequence of hour, minute, and second from left to right.	
Tag	Route tag	

display ip routing-table acl

Syntax

display ip routing-table acl *acl-number* [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

acl-number: Basic ACL number, in the range of 2000 to 2999.

verbose: Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only brief information about active routes.

Description

Use the **display ip routing-table acl** command to display information about routes permitted by a specified basic ACL.

This command is intended for the follow-up display of routing policies.

For more information about routing policy, refer to *Routing Policy Configuration* in the *IP Routing Volume*.

Note

If the specified ACL does not exist or it has no rules configured, the entire routing table is displayed.

Examples

Define basic ACL 2000 and set the route filtering rules.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule deny source any
```

Display brief information about active routes permitted by basic ACL 2000.

```
[Sysname-acl-basic-2000] display ip routing-table acl 2000
Routes Matched by Access list : 2000
Summary Count : 6

Destination/Mask    Proto  Pre  Cost        NextHop      Interface

10.1.1.0/24         Direct 0    0           10.1.1.2     Vlan1
10.1.1.2/32         Direct 0    0           127.0.0.1    InLoop0
10.1.2.0/24         Direct 0    0           10.1.2.1     Vlan2
10.1.2.1/32         Direct 0    0           127.0.0.1    InLoop0
10.1.3.0/24         Direct 0    0           10.1.3.1     Vlan3
10.1.3.1/32         Direct 0    0           127.0.0.1    InLoop0
```

For detailed description of the above output, see Table 1-1.

Display detailed information about both active and inactive routes permitted by basic ACL 2000.

```
<Sysname> display ip routing-table acl 2000 verbose
Routes Matched by Access list : 2000
Summary Count: 6

Destination: 10.1.1.0/24
```

```
     Protocol: Direct        Process ID: 0
   Preference: 0                 Cost: 0
      NextHop: 10.1.1.2       Interface: Vlan-interface1
  RelyNextHop: 0.0.0.0        Neighbour: 0.0.0.0
    Tunnel ID: 0x0               Label: NULL
        State: Active Adv          Age: 00h25m32s
          Tag: 0

Destination: 10.1.1.2/32
     Protocol: Direct        Process ID: 0
   Preference: 0                 Cost: 0
      NextHop: 127.0.0.1      Interface: InLoopBack0
  RelyNextHop: 0.0.0.0        Neighbour: 0.0.0.0
    Tunnel ID: 0x0               Label: NULL
        State: Active NoAdv        Age: 00h41m34s
          Tag: 0

Destination: 10.1.2.0/24
     Protocol: Direct        Process ID: 0
   Preference: 0                 Cost: 0
      NextHop: 10.1.2.1       Interface: Vlan-interface2
  RelyNextHop: 0.0.0.0        Neighbour: 0.0.0.0
    Tunnel ID: 0x0               Label: NULL
        State: Active Adv          Age: 00h05m42s
          Tag: 0

Destination: 10.1.2.1/32
     Protocol: Direct        Process ID: 0
   Preference: 0                 Cost: 0
      NextHop: 127.0.0.1      Interface: InLoopBack0
  RelyNextHop: 0.0.0.0        Neighbour: 0.0.0.0
    Tunnel ID: 0x0               Label: NULL
        State: Active NoAdv        Age: 00h05m42s
          Tag: 0

Destination: 10.1.3.0/24
     Protocol: Direct        Process ID: 0
   Preference: 0                 Cost: 0
      NextHop: 10.1.3.1       Interface: Vlan-interface3
  RelyNextHop: 0.0.0.0        Neighbour: 0.0.0.0
    Tunnel ID: 0x0               Label: NULL
        State: Active Adv          Age: 00h05m31s
          Tag: 0

Destination: 10.1.3.1/32
     Protocol: Direct        Process ID: 0
   Preference: 0                 Cost: 0
      NextHop: 127.0.0.1      Interface: InLoopBack0
```

```
RelyNextHop: 0.0.0.0        Neighbour: 0.0.0.0
  Tunnel ID: 0x0              Label: NULL
      State: Active NoAdv       Age: 00h05m32s
        Tag: 0
```

For the description of the command output above, see Table 1-2.

display ip routing-table *ip-address*

Syntax

display ip routing-table *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]

display ip routing-table *ip-address1* { *mask-length* | *mask* } *ip-address2* { *mask-length* | *mask* } [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

ip-address: Destination IP address, in dotted decimal format.

mask-length: IP address mask length in the range 0 to 32.

mask: IP address mask in dotted decimal format.

longer-match: Displays the route with the longest mask.

verbose: Displays detailed routing table information, including both active and inactive routes. With this argument absent, the command displays only brief information about active routes.

Description

Use the **display ip routing-table** *ip-address* command to display information about routes to a specified destination address.

Executing the command with different parameters yields different output:

- **display ip routing-table** *ip-address*

The system ANDs the input destination IP address with the subnet mask in each route entry; and ANDs the destination IP address in each route entry with its corresponding subnet mask.

If the two operations yield the same result for an entry and this entry is active, it is displayed.

- **display ip routing-table** *ip-address mask*

The system ANDs the input destination IP address with the input subnet mask; and ANDs the destination IP address in each route entry with the input subnet mask.

If the two operations yield the same result for an entry and the entry is active with a subnet mask less than or equal to the input subnet mask, the entry is displayed.

Only route entries that exactly match the input destination address and mask are displayed.

- **display ip routing-table** *ip-address* **longer-match**

The system ANDs the input destination IP address with the subnet mask in each route entry; and ANDs the destination IP address in each route entry with its corresponding subnet mask.

If the two operations yield the same result for multiple entries that are active, the one with longest mask length is displayed.

- **display ip routing-table** *ip-address mask* **longer-match**

The system ANDs the input destination IP address with the input subnet mask; and ANDs the destination IP address in each route entry with the input subnet mask.

If the two operations yield the same result for multiple entries with a mask less than or equal to the input subnet mask, the one that is active with longest mask length is displayed.

Use the **display ip routing-table** *ip-address1* { *mask-length* | *mask* } *ip-address2* { *mask-length* | *mask* } command to display route entries with destination addresses within a specified range.

Examples

Display route entries for the destination IP address 11.1.1.1.

```
<Sysname> display ip routing-table 11.1.1.1
Routing Table : Public
Summary Count : 4

Destination/Mask    Proto  Pre  Cost        NextHop         Interface

0.0.0.0/0           Static 60   0           0.0.0.0         NULL0
11.0.0.0/8          Static 60   0           0.0.0.0         NULL0
11.1.0.0/16         Static 60   0           0.0.0.0         NULL0
11.1.1.0/24         Static 60   0           0.0.0.0         NULL0
```

For detailed description about the output, see Table 1-1.

Display route entries by specifying a destination IP address and the **longer-match** keyword.

```
[Sysname] display ip routing-table 11.1.1.1 longer-match
Routing Table : Public
Summary Count : 1

Destination/Mask    Proto  Pre  Cost        NextHop         Interface

11.1.1.0/24         Static 60   0           0.0.0.0         NULL0
```

Display route entries by specifying a destination IP address and mask.

```
[Sysname] display ip routing-table 11.1.1.1 24
Routing Table : Public
Summary Count : 3

Destination/Mask    Proto  Pre  Cost        NextHop         Interface

11.0.0.0/8          Static 60   0           0.0.0.0         NULL0
11.1.0.0/16         Static 60   0           0.0.0.0         NULL0
11.1.1.0/24         Static 60   0           0.0.0.0         NULL0
```

Display route entries by specifying a destination IP address and mask and the **longer-match** keyword.

```
[Sysname] display ip routing-table 11.1.1.1 24 longer-match
Routing Table : Public
```

```
Summary Count : 1
Destination/Mask    Proto  Pre  Cost        NextHop         Interface
11.1.1.0/24         Static 60   0           0.0.0.0         NULL0
```

For detailed description of the above output, see Table 1-1.

Display route entries for destination addresses in the range 1.1.1.0 to 5.5.5.0.

```
<Sysname> display ip routing-table 1.1.1.0 24 5.5.5.0 24
Routing Table : Public

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
1.1.1.0/24          Direct 0    0           1.1.1.1         Vlan1
1.1.1.1/32          Direct 0    0           127.0.0.1       InLoop0
2.2.2.0/24          Direct 0    0           2.2.2.1         Vlan2
2.2.2.1/32          Direct 0    0           127.0.0.1       InLoop0
```

display ip routing-table ip-prefix

Syntax

display ip routing-table ip-prefix *ip-prefix-name* [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

ip-prefix-name: IP prefix list name, a string of 1 to 19 characters.

verbose: Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only brief information about active routes.

Description

Use the **display ip routing-table ip-prefix** command to display information about routes permitted by a specified prefix list.

This command is intended for the follow-up display of routing policies. If the specified prefix list is not configured, detailed information about all routes (with the **verbose** keyword) or brief information about all active routes (without the **verbose** keyword) is displayed.

Examples

Configure a prefix list named **test**, permitting routes with a prefix of 2.2.2.0 and a mask length between 24 and 32.

```
<Sysname> system-view
[Sysname] ip ip-prefix test permit 2.2.2.0 24 less-equal 32
```

Display brief information about active routes permitted by the prefix list **test**.

```
[Sysname] display ip routing-table ip-prefix test
Routes Matched by Prefix list : test
Summary Count : 2
```

```
Destination/Mask   Proto  Pre  Cost      NextHop         Interface
2.2.2.0/24         Direct  0    0         2.2.2.1         Vlan2
2.2.2.1/32         Direct  0    0         127.0.0.1       InLoop0
```

For detailed description of the above output, see Table 1-1.

Display detailed information about both active and inactive routes permitted by IP prefix list **test**.

```
[Sysname] display ip routing-table ip-prefix test verbose
Routes Matched by Prefix list  test :
Summary Count : 2

Destination: 2.2.2.0/24
    Protocol: Direct              Process ID: 0
  Preference: 0                       Cost: 0
     NextHop: 2.2.2.1             Interface: Vlan-interface2
 RelyNextHop: 0.0.0.0              Neighbour: 0.0.0.0
   Tunnel ID: 0x0                     Label: NULL
       State: Active Adv               Age: 00h20m52s
         Tag: 0

Destination: 2.2.2.1/32
    Protocol: Direct              Process ID: 0
  Preference: 0                       Cost: 0
     NextHop: 127.0.0.1           Interface: InLoopBack0
 RelyNextHop: 0.0.0.0              Neighbour: 0.0.0.0
   Tunnel ID: 0x0                     Label: NULL
       State: Active NoAdv             Age: 00h20m52s
         Tag: 0
```

For detailed description of the above output, see Table 1-2.

display ip routing-table protocol

Syntax

display ip routing-table protocol *protocol* [**inactive** | **verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

protocol: Routing protocol. It can be **direct**, **rip**, or **static**.

inactive: Displays information about only inactive routes. With this argument absent, the command displays information about both active and inactive routes.

verbose: Displays detailed routing table information. With this argument absent, the command displays brief routing table information.

Description

Use the **display ip routing-table protocol** command to display routing information of a specified routing protocol.

Examples

Display brief information about direct routes.

```
<Sysname> display ip routing-table protocol direct
Public Routing Table : Direct
Summary Count : 4

Direct Routing table Status : < Active>
Summary Count :  4

Destination/Mask    Proto  Pre  Cost      NextHop         Interface
2.2.2.0/24          Direct 0    0         2.2.2.1         Vlan2
2.2.2.2/32          Direct 0    0         127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0         127.0.0.1       InLoop0
127.0.0.1/32          Direct 0    0         127.0.0.1       InLoop0

Direct Routing table Status : < Inactive>
Summary Count : 0
```

Display brief information about static routes.

```
<Sysname> display ip routing-table protocol static
Public Routing Table : Static
Summary Count : 1

Static Routing table Status : < Active>
Summary Count :  0

Static Routing table Status : < Inactive>
Summary Count : 1
Destination/Mask    Proto   Pre  Cost      NextHop     Interface
1.2.3.0/24          Static  60   0         1.2.4.5     Vlan10
```

For detailed description of the above output, see Table 1-1.

display ip routing-table statistics

Syntax

display ip routing-table statistics

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ip routing-table statistics** command to display the route statistics of the routing table.

Examples

Display route statistics in the routing table.

```
<Sysname> display ip routing-table statistics
Proto     route      active     added      deleted      freed
DIRECT    24         4          25         1            0
STATIC    4          1          4          0            0
Total     28         5          29         1            0
```

Table 1-3 display ip routing-table statistics command output description

Field	Description
Proto	Origin of the routes.
route	Number of routes from the origin
active	Number of active routes from the origin
added	Number of routes added into the routing table since the router started up or the routing table was last cleared
deleted	Number of routes marked as deleted, which will be freed after a period.
freed	Number of routes that got freed, that is, got removed permanently.
Total	Total number

display ipv6 routing-table

Syntax

display ipv6 routing-table

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ipv6 routing-table** command to display brief routing table information, including destination IP address and prefix, protocol type, priority, metric, next hop and outbound interface.

The command displays only active routes, namely, the brief information about the current optimal routes.

Examples

Display brief routing table information

```
<Sysname> display ipv6 routing-table
Routing Table :
       Destinations : 1       Routes : 1

Destination : ::1/128                    Protocol    : Direct
NextHop     : ::1                        Preference  : 0
Interface   : InLoop0                    Cost        : 0
```

Table 1-4 display ipv6 routing-table command output description

Field	Description
Destination	IPv6 address of the destination network/host
NextHop	Nexthop address
Preference	Route priority
Interface	Outbound interface
Protocol	Routing protocol
Cost	Route cost

display ipv6 routing-table acl

Syntax

display ipv6 routing-table acl *acl6-number* [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

acl6-number: Basic IPv6 ACL number, in the range 2000 to 2999.

verbose: Displays both active and inactive verbose routing information permitted by the ACL. Without this keyword, only brief active routing information is displayed.

Description

Use the **display ipv6 routing-table acl** command to display routing information permitted by the IPv6 ACL.

If the specified IPv6 ACL is not available, all routing information is displayed.

Examples

Display brief routing information permitted by ACL 2000.

```
<Sysname> display ipv6 routing-table acl 2000
Routes Matched by Access list  2000  :
Summary Count : 2

Destination : ::1/128                    Protocol   : Direct
NextHop     : ::1                       Preference : 0
Interface   : InLoop0                    Cost       : 0
Destination : 1:1::/64                   Protocol   : Static
NextHop     : ::                        Preference : 60
Interface   : NULL0                      Cost       : 0
```

Refer to Table 1-4 for description about the above output.

display ipv6 routing-table *ipv6-address*

Syntax

display ipv6 routing-table *ipv6-address prefix-length* [**longer-match**] [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-address: Destination IPv6 address.

prefix-length: Prefix length, in the range 0 to 128.

longer-match: Displays the matched route having the longest prefix length.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description

Use the **display ipv6 routing-table** *ipv6-address* command to display routing information about the specified destination IPv6 address.

Executing the command with different parameters yields different output:

- **display ipv6 routing-table** *ipv6-address prefix-length*

The system ANDs the input destination IPv6 address with the input prefix length, and ANDs the destination IPv6 address in each route entry with the input prefix length.

If the two operations yield the same result for an entry and the entry is active with a prefix length less than or equal to the input prefix length, the entry is displayed.

Only route entries that exactly match the input destination address and prefix length are displayed.

- **display ipv6 routing-table** *ipv6-address prefix-length* **longer-match**

The system ANDs the input destination IPv6 address with the input prefix length; and ANDs the destination IPv6 address in each route entry with the input prefix length.

If the two operations yield the same result for multiple entries with a prefix length less than or equal to the input prefix length, the one that is active with the longest prefix length is displayed.

Examples

Display brief information about the route matching the specified destination IPv6 address.

```
<Sysname> display ipv6 routing-table 10::1 127
Routing Table:
Summary Count: 3

Destination: 10::/64                              Protocol  : Static
NextHop    : ::                                  Preference: 60
Interface  : NULL0                               Cost      : 0

Destination: 10::/68                              Protocol  : Static
NextHop    : ::                                  Preference: 60
Interface  : NULL0                               Cost      : 0

Destination: 10::/120                             Protocol  : Static
NextHop    : ::                                  Preference: 60
Interface  : NULL0                               Cost      : 0
```

Display brief information about the matched route with the longest prefix length.

```
<Sysname> display ipv6 routing-table 10:: 127 longer-match
Routing Tables:
Summary Count : 1
Destination: 10::/120                             Protocol  : Static
NextHop    : ::                                  Preference: 60
Interface  : NULL0                               Cost      : 0
```

Refer to Table 1-4 for description about the above output.

display ipv6 routing-table *ipv6-address1 ipv6-address2*

Syntax

display ipv6 routing-table *ipv6-address1 prefix-length1 ipv6-address2 prefix-length2* [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-address1/*ipv6-address2*: An IPv6 address range from IPv6 address1 to IPv6 address2.

prefix-length1/*prefix-length2*: Prefix length, in the range 0 to 128.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description

Use the **display ipv6 routing-table** *ipv6-address1 ipv6-address2* command to display routes with destinations falling into the specified IPv6 address range.

Examples

Display routes with destinations falling into the IPv6 address range.

```
<Sysname> display ipv6 routing-table 100:: 64 300:: 64
Routing Table :
Summary Count : 3

Destination: 100::/64                          Protocol  : Static
NextHop    : ::                               Preference: 60
Interface  : NULL0                             Cost      : 0

Destination: 200::/64                          Protocol  : Static
NextHop    : ::                               Preference: 60
Interface  : NULL0                             Cost      : 0

Destination: 300::/64                          Protocol  : Static
NextHop    : ::                               Preference: 60
Interface  : NULL0                             Cost      : 0
```

Refer to Table 1-4 for description about the above output.

display ipv6 routing-table ipv6-prefix

Syntax

display ipv6 routing-table ipv6-prefix *ipv6-prefix-name* [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

ipv6-prefix-name: Name of the IPv6 prefix list, in the range 1 to 19 characters.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description

Use the **display ipv6 routing-table ipv6-prefix** command to display routes permitted by the IPv6 prefix list.

Examples

Display brief active routing information permitted by the IPv6 prefix list **test2**.

```
<Sysname> display ipv6 routing-table ipv6-prefix test2
Routes Matched by Prefix list  test2  :
Summary Count : 1

Destination: 100::/64                              Protocol  : Static
NextHop    : ::                                  Preference: 60
Interface  : NULL0                               Cost      : 0
```

Refer to Table 1-4 for description about the above output.

display ipv6 routing-table protocol

Syntax

display ipv6 routing-table protocol *protocol* [**inactive** | **verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

protocol: Displays routes of a routing protocol, which can be **direct**, **ripng** and **static**.

inactive: Displays only inactive routes. Without the keyword, all active and inactive routes are displayed.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description

Use the **display ipv6 routing-table protocol** command to display routes of a specified routing protocol.

Examples

Display brief information about all direct routes.

```
<Sysname> display ipv6 routing-table protocol direct
Direct Routing Table :
Summary Count : 1

Direct Routing Table's Status : < Active >
Summary Count : 1

Destination: ::1/128                               Protocol  : Direct
NextHop    : ::1                                 Preference: 0
Interface  : InLoop0                             Cost      : 0
```

```
Direct Routing Table's Status : < Inactive >
Summary Count : 0
```

Refer to Table 1-4 for description about the above output.

display ipv6 routing-table statistics

Syntax

display ipv6 routing-table statistics

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ipv6 routing-table statistics** command to display routing statistics, including total route number, added route number and deleted route number.

Examples

Display routing statistics.

```
<Sysname> display ipv6 routing-table statistics
Protocol   route     active    added     deleted    freed
DIRECT     1         1         1         0          0
STATIC     3         0         3         0          0
Total      4         1         4         0          0
```

Table 1-5 display ipv6 routing-table statistics command output description

Field	Description
Protocol	Routing protocol
route	Route number of the protocol
active	Number of active routes
added	Routes added after the last startup of the router
deleted	Deleted routes, which will be released after a specified time
freed	Released (totally removed from the routing table) route number
Total	Total number of routes

display ipv6 routing-table verbose

Syntax

display ipv6 routing-table verbose

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ipv6 routing-table verbose** command to display detailed information about all active and inactive routes, including the statistics of the entire routing table and information for each route.

Examples

Display detailed information about all active and inactive routes.

```
<Sysname> display ipv6 routing-table verbose
Routing Table :
       Destinations : 1      Routes : 1

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 RelayNextHop : ::                           Tag          : 0H
 Neighbour    : ::                           ProcessID    : 0
 Interface    : InLoopBack0                     Protocol     : Direct
 State        : Active NoAdv                 Cost         : 0
 Tunnel ID    : 0x0                          Label        : NULL
 Age          : 22161sec
```

Table 1-6 display ipv6 routing-table verbose command output description

Field	Description
Destination	Destination IPv6 address
PrefixLength	Prefix length of the address
Nexthop	Next hop
Preference	Route priority
RelayNextHop	Recursive next hop
Tag	Tag of the route
Neighbour	Neighbor address
ProcessID	Process ID
Interface	Outbound interface
Protocol	Routing protocol
State	State of the route, Active, Inactive, Adv (advertised), or NoAdv (not advertised)
Cost	Cost of the route

Field	Description
Tunnel ID	Tunnel ID
Label	Label
Age	Time that has elapsed since the route was generated

reset ip routing-table statistics protocol

Syntax

reset ip routing-table statistics protocol { *protocol* | **all** }

View

User view

Default Level

2: System level

Parameters

protocol: Clears statistics for the IPv4 routing protocol, which can be **direct**, **rip**, or **static**.

all: Clears statistics for all IPv4 routing protocols.

Description

Use the **reset ip routing-table statistics protocol** command to clear routing statistics for the routing table.

Examples

Clear all the routing statistics information.

```
<Sysname> reset ip routing-table statistics protocol all
```

reset ipv6 routing-table statistics

Syntax

reset ipv6 routing-table statistics protocol { *protocol* | **all** }

View

User view

Default Level

2: System level

Parameters

protocol: Clears statistics for the routing protocol, which can be **direct**, **ripng**, or **static**.

all: Clears statistics for all IPv6 routing protocols.

Description

Use the **reset ipv6 routing-table statistics** command to clear the route statistics of the routing table.

Examples

Clear statistics for all routing protocols.

```
<Sysname> reset ipv6 routing-table statistics protocol all
```

2 Static Routing Configuration Commands

Note

The term “router” in this document refers to a router in a generic sense or a Layer 3 switch.

Static Routing Configuration Commands

delete static-routes all

Syntax

delete static-routes all

View

System view

Default Level

2: System level

Parameters

None.

Description

Use the **delete static-routes all** command to delete all static routes.

When you use this command to delete static routes, the system will prompt you to confirm the operation before deleting all the static routes.

Related commands: **ip route-static** and **display ip routing-table** in *IP Routing Table Display Commands* in the *IP Routing Volume*.

Examples

Delete all static routes on the router.

```
<Sysname> system-view
[Sysname] delete static-routes all
This will erase all ipv4 static routes and their configurations, you must reconf
igure all static routes
Are you sure?[Y/N]:Y
```

ip route-static

Syntax

ip route-static *dest-address* { *mask* | *mask-length* } { *next-hop-address* [**track** *track-entry-number*] | *interface-type interface-number next-hop-address*] } [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]

undo ip route-static *dest-address* { *mask* | *mask-length* } [*next-hop-address* | *interface-type interface-number* [*next-hop-address*]] [**preference** *preference-value*]

View

System view

Default Level

2: System level

Parameters

dest-address: Destination IP address of the static route, in dotted decimal notation.

mask: Mast of the IP address, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

next-hop-address: IP address of the next hop, in dotted decimal notation.

interface-type interface-number: Specifies the output interface by its type and number.

preference *preference-value* : Specifies the preference of the static route, which is in the range of 1 to 255 and defaults to 60.

tag *tag-value*: Sets a tag value for the static route from 1 to 4294967295. The default is 0. Tags of routes are used in routing policies to control routing.

description *description-text*: Configures a description for the static route, which consists of 1 to 60 characters, including special characters like space, but excluding **?**.

track *track-entry-number*: Associates the static route with a track entry. Use the *track-entry-number* argument to specify a track entry number, in the range 1 to 1024.

Description

Use the **ip route-static** command to configure a unicast static route.

Use the **undo ip route-static** command to delete a unicast static route.

When configuring a unicast static route, note that:

1) If the destination IP address and the mask are both 0.0.0.0, the configured route is a default route. If routing table searching fails, the router will use the default route for packet forwarding.
2) Different route management policies can be implemented for different route preference configurations. For example, specifying the same preference for different routes to the same destination address enables load sharing, while specifying different preferences for these routes enables route backup.
3) When configuring a static route, Note that the next hop address must not be the IP address of the local interface; otherwise, the route configuration will not take effect. When specifying the output interface, note that: for a Null 0 or loopback interface, if the output interface has already been configured, there is no need to configure the next hop address.

Related commands: **display ip routing-table**, **ip route-static default-preference**.

Note

- To configure track monitoring for an existing static route, simply associate the static route with a track entry. For a non-existent static route, configure it and associate it with a Track entry.
- If a static route needs route recursion, the associated track entry must monitor the nexthop of the recursive route instead of that of the static route; otherwise, a valid route may be mistakenly considered invalid.

Examples

Configure a static route, whose destination address is 1.1.1.1/24, next hop address is 2.2.2.2, tag value is 45, and description information is **for internet & intranet**.

```
<Sysname> system-view
[Sysname] ip route-static 1.1.1.1 24 2.2.2.2 tag 45 description for internet & intranet
```

ip route-static default-preference

Syntax

ip route-static default-preference *default-preference-value*

undo ip route-static default-preference

View

System view

Default Level

2: System level

Parameters

default-preference-value: Default preference for static routes, which is in the range of 1 to 255.

Description

Use the **ip route-static default-preference** command to configure the default preference for static routes.

Use the **undo ip route-static default-preference** command to restore the default.

By default, the default preference of static routes is 60.

Note that:

- If no preference is specified when configuring a static route, the default preference is used.
- When the default preference is re-configured, it applies to newly added static routes only.

Related commands: **ip route-static** and **display ip routing-table** in *IP Routing Table Display Commands* in the *IP Routing Volume*.

Examples

Set the default preference of static routes to 120.

```
<Sysname> system-view
[Sysname] ip route-static default-preference 120
```

3 IPv6 Static Routing Configuration Commands

Throughout this chapter, the term “router” refers to a router in a generic sense or a Layer 3 switch running routing protocols.

IPv6 Static Routing Configuration Commands

delete ipv6 static-routes all

Syntax

delete ipv6 static-routes all

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **delete ipv6 static-routes all** command to delete all static routes including the default route.

When using this command, you will be prompted whether to continue the deletion and only after you confirm the deletion will the static routes be deleted.

Related commands: **display ipv6 routing-table**, **ipv6 route-static**.

Examples

Delete all IPv6 static routes.

```
<Sysname> system-view
[Sysname] delete ipv6 static-routes all
This will erase all ipv6 static routes and their configurations, you must reconfigure all
static routes
Are you sure?[Y/N]Y
```

ipv6 route-static

Syntax

ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number*] *nexthop-address* [**preference** *preference-value*]

undo ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number*] [*nexthop-address*] [**preference** *preference-value*]

View

System view

Default Level

2: System level

Parameters

ipv6-address prefix-length: IPv6 address and prefix length.

interface-type interface-number: Interface type and interface number of the output interface.

nexthop-address: Next hop IPv6 address.

preference-value: Route preference value, in the range of 1 to 255. The default is 60.

Description

Use the **ipv6 route-static** command to configure an IPv6 static route.

Use the **undo ipv6 route-static** command to remove an IPv6 static route.

An IPv6 static route that has the destination address configured as **::/0** (a prefix length of 0) is the default IPv6 route. If the destination address of an IPv6 packet does not match any entry in the routing table, this default route will be used to forward the packet.

Related commands: **display ipv6 routing-table**, **delete ipv6 static-routes all**.

Examples

Configure a static IPv6 route, with the destination address being 1:1:2::/24 and next hop being 1:1:3::1.

```
<Sysname> system-view
[Sysname] ipv6 route-static 1:1:2:: 24 1:1:3::1
```

Table of Contents

1 IGMP Snooping Configuration Commands

IGMP Snooping Configuration Commands

display igmp-snooping group

Syntax

display igmp-snooping group [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the IGMP Snooping multicast group information in the specified VLAN, where *vlan-id* is in the range of 1 to 4094. If you do not specify a VLAN, this command will display the IGMP Snooping multicast group information in all VLANs.

slot *slot-number*: Displays information about IGMP Snooping multicast groups on the specified IRF member device. The *slot-number* argument is the member number of the device in the IRF, which you can display with the **display irf** command. The value range for the *slot-number* argument depends on the number of members and numbering conditions in the current IRF. If no IRF exists, the *slot-number* argument is the current device number.

verbose: Specifies to display the detailed IGMP Snooping multicast group information.

Description

Use the **display igmp-snooping group** command to view the IGMP Snooping multicast group information.

Examples

View the detailed IGMP Snooping multicast group information in VLAN 2.

```
<Sysname> display igmp-snooping group vlan 2 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).
  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):2.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
    Total 1 MAC Group(s).
```

```
Router port(s):total 1 port.
       GE1/0/1             (D) ( 00:01:30 )
IP group(s):the following ip group(s) match to one mac group.
  IP group address:224.1.1.1
    (0.0.0.0, 224.1.1.1):
      Attribute:    Host Port
      Host port(s):total 1 port.
        GE1/0/2             (D) ( 00:03:23 )
MAC group(s):
  MAC group address:0100-5e01-0101
      Host port(s):total 1 port.
        GE1/0/2
```

Table 1-1 display igmp-snooping group command output description

Field	Description
Total 1 IP Group(s).	Total number of IP multicast groups
Total 1 IP Source(s).	Total number of multicast sources
Total 1 MAC Group(s).	Total number of MAC multicast groups
Port flags: D-Dynamic port, S-Static port, C-Copy port	Port flags: D for dynamic port, S for static port, C for port copied from a (*, G) entry to an (S, G) entry
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: R for real egress sub-VLAN under the current entry, C for sub-VLAN copied from a (*, G) entry to an (S, G) entry
Router port(s)	Number of router ports
(00:01:30)	Remaining time of the dynamic member port or router port aging timer.
IP group address	Address of IP multicast group
(0.0.0.0, 224.1.1.1)	An (S, G), where 0.0.0.0 implies any multicast source
MAC group address	Address of MAC multicast group
Attribute	Attribute of IP multicast group
Host port(s)	Number of member ports

display igmp-snooping statistics

Syntax

display igmp-snooping statistics

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display igmp-snooping statistics** command to view the statistics information of IGMP messages learned by IGMP Snooping.

Examples

View the statistics information of IGMP messages learned by IGMP Snooping.

```
<Sysname> display igmp-snooping statistics
  Received IGMP general queries:0.
  Received IGMPv1 reports:0.
  Received IGMPv2 reports:19.
  Received IGMP leaves:0.
  Received IGMPv2 specific queries:0.
  Sent    IGMPv2 specific queries:0.
  Received IGMPv3 reports:1.
  Received IGMPv3 reports with right and wrong records:0.
  Received IGMPv3 specific queries:0.
  Received IGMPv3 specific sg queries:0.
  Sent    IGMPv3 specific queries:0.
  Sent    IGMPv3 specific sg queries:0.
  Received error IGMP messages:19.
```

Table 1-2 display igmp-snooping statistics command output description

Field	Description
general queries	General query messages
specific queries	Group-specific query messages
reports	Report messages
leaves	Leave messages
reports with right and wrong records	Report messages with correct and incorrect records
specific sg query packet(s)	Group-and-source-specific query message(s)
error IGMP messages	IGMP messages with errors

fast-leave (IGMP-Snooping view)

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

View

IGMP-Snooping view

Default Level

2: System level

Parameters

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **fast-leave** command to enable fast leave processing globally. With this function enabled, when the switch receives an IGMP leave message on a port, it directly removes that port from the multicast forwarding entry of the specific group.

Use the **undo fast-leave** command to disable fast leave processing globally.

By default, fast leave processing is disabled.

Note that:

- This command works on IGMP Snooping–enabled VLANs.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

Related commands: **igmp-snooping fast-leave**.

Examples

Enable fast leave processing globally in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] fast-leave vlan 2
```

group-policy (IGMP-Snooping view)

Syntax

group-policy *acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

View

IGMP-Snooping view

Default Level

2: System level

Parameters

acl-number: Basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL rule is used to match the multicast source address(es) specified in IGMPv3 reports, rather than the source address in the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS_EX or TO_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **group-policy** command to configure a global multicast group filter, namely to control the multicast groups a host can join.

Use the **undo group-policy** command to remove the configured global multicast group filter.

By default, no global multicast group filter is configured, namely a host can join any valid multicast group.

Note that:

- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.
- If the specified ACL does not exist or the ACL rule is null, all multicast groups will be filtered out.
- You can configure different ACL rules for a port in different VLANs; for a given VLAN, a newly configured ACL rule will override the existing one.

Related commands: **igmp-snooping group-policy**.

Examples

Apply ACL 2000 as a multicast group filter in VLAN 2 so that hosts in this VLAN can join 225.1.1.1 only.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] igmp-snooping
[Sysname-igmp-snooping] group-policy 2000 vlan 2
```

host-aging-time (IGMP-Snooping view)

Syntax

host-aging-time *interval*

undo host-aging-time

View

IGMP-Snooping view

Default Level

2: System level

Parameters

interval: Dynamic member port aging time, in seconds. The effective range is 200 to 1,000.

Description

Use the **host-aging-time** command to configure the aging time of dynamic member ports globally.

Use the **undo host-aging-time** command to restore the default setting.

By default, the aging time of dynamic member ports is 260 seconds.

This command works on IGMP Snooping–enabled VLANs.

Related commands: **igmp-snooping host-aging-time**.

Examples

Set the aging time of dynamic member ports globally to 300 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] host-aging-time 300
```

igmp-snooping

Syntax

igmp-snooping

undo igmp-snooping

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **igmp-snooping** command to enable IGMP Snooping globally and enter IGMP-Snooping view.

Use the **undo igmp-snooping** command to disable IGMP Snooping globally.

By default, IGMP Snooping is disabled.

Related commands: **igmp-snooping enable**.

Examples

Enable IGMP Snooping globally and enter IGMP-Snooping view.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping]
```

igmp-snooping drop-unknown

Syntax

igmp-snooping drop-unknown

undo igmp-snooping drop-unknown

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **igmp-snooping drop-unknown** command to enable the function of dropping unknown multicast data in the current VLAN,so that such multicast data will only be forwarded to router ports.

Use the **undo igmp-snooping drop-unknown** command to disable the function of dropping unknown multicast data in the current VLAN.

By default, this function is disabled, that is, unknown multicast data is flooded.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Examples

In VLAN 2, enable the function of dropping unknown multicast data.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping drop-unknown
```

igmp-snooping enable

Syntax

igmp-snooping enable

undo igmp-snooping enable

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **igmp-snooping enable** command to enable IGMP Snooping in the current VLAN.

Use the **undo igmp-snooping enable** command to disable IGMP Snooping in the current VLAN.

By default, IGMP Snooping is disabled in a VLAN.

IGMP Snooping must be enabled globally before it can be enabled in a VLAN.

Related commands: **igmp-snooping**.

Examples

Enable IGMP Snooping in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
```

igmp-snooping fast-leave

Syntax

igmp-snooping fast-leave [**vlan** *vlan-list*]

undo igmp-snooping fast-leave [**vlan** *vlan-list*]

View

Ethernet port view, Layer 2 aggregate port view, port group view

Default Level

2: System level

Parameters

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **igmp-snooping fast-leave** command to enable fast leave processing on the current port or group of ports. With this function enabled, when the switch receives an IGMP leave message on a port, it directly removes that port from the multicast forwarding entry of the specific group.

Use the **undo igmp-snooping fast-leave** command to disable fast leave processing on the current port or group of ports.

By default, fast leave processing is disabled.

Note that:

- This command works on IGMP Snooping–enabled VLANs.
- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).

Related commands: **fast-leave**.

Examples

Enable fast leave processing on GigabitEthernet1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping fast-leave vlan 2
```

igmp-snooping general-query source-ip

Syntax

igmp-snooping general-query source-ip { **current-interface** | *ip-address* }

undo igmp-snooping general-query source-ip

View

VLAN view

Default Level

2: System level

Parameters

current-interface: Sets the source address of IGMP general queries to the address of the current VLAN interface. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 will be used as the source IP address of IGMP general queries.

ip-address: Specifies the source address of IGMP general queries, which can be any legal IP address.

Description

Use the **igmp-snooping general-query source-ip** command to configure the source address of IGMP general queries.

Use the **undo igmp-snooping general-query source-ip** command to restore the default configuration.

By default, the source IP address of IGMP general queries is 0.0.0.0.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Examples

In VLAN 2 specify 10.1.1.1 as the source IP address of IGMP general queries.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping general-query source-ip 10.1.1.1
```

igmp-snooping group-limit

Syntax

igmp-snooping group-limit *limit* [**vlan** *vlan-list*]

undo igmp-snooping group-limit [**vlan** *vlan-list*]

View

Ethernet port view, Layer 2 aggregate port view, port group view

Default Level

2: System level

Parameters

limit: Maximum number of multicast groups that can be joined on a port. The effective range is 1 to 1000.

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **igmp-snooping group-limit** command to configure the maximum number of multicast groups that can be joined on a port.

Use the **undo igmp-snooping group-limit** command to restore the default setting.

The default the maximum number of multicast groups is 1000.

Note that:

- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).

Examples

Specify to allow a maximum of 10 multicast groups to be joined on GigabitEthernet1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-limit 10 vlan 2
```

igmp-snooping group-policy

Syntax

igmp-snooping group-policy *acl-number* [**vlan** *vlan-list*]

undo igmp-snooping group-policy [**vlan** *vlan-list*]

View

Ethernet port view, Layer 2 aggregate port view, port group view

Default Level

2: System level

Parameters

acl-number: Basic or advanced ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced ACL rule is used to match the multicast source address(es) specified in IGMPv3 reports, rather than the source address in the IP packets. The system assumes that an IGMPv1 or IGMPv2 report or an IGMPv3 IS_EX and TO_EX report that does not carry a multicast source address carries a multicast source address of 0.0.0.0.

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **igmp-snooping group-policy** command to configure a multicast group filter on the current port(s), namely to control the multicast groups hosts on the port(s) can join.

Use the **undo igmp-snooping group-policy** command to remove a multicast group filter on the current port(s).

By default, no multicast group filter is configured on a port, namely a host can join any valid multicast group.

Note that:

- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).
- If the specified ACL does not exist or the ACL rule is null, all multicast groups will be filtered out.
- You can configure different ACL rules for a port in different VLANs; for a given VLAN, a newly configured ACL rule will override the existing one.

Related commands: **group-policy**.

Examples

Apply ACL 2000 as a multicast group filter so that hosts on GigabitEthernet 1/0/1 in VLAN 2 can join 225.1.1.1 only.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2
```

igmp-snooping host-aging-time

Syntax

igmp-snooping host-aging-time *interval*

undo igmp-snooping host-aging-time

View

VLAN view

Default Level

2: System level

Parameters

interval: Dynamic member port aging time, in seconds. The effective range is 200 to 1,000.

Description

Use the **igmp-snooping host-aging-time** command to configure the aging time of dynamic member ports in the current VLAN.

Use the **undo igmp-snooping host-aging-time** command to restore the default setting.

By default, the aging time of dynamic member ports is 260 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **host-aging-time**.

Examples

Set the aging time of dynamic member ports to 300 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping host-aging-time 300
```

igmp-snooping host-join

Syntax

igmp-snooping host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

View

Ethernet port view, Layer 2 aggregate port view, port group view

Default Level

2: System level

Parameters

group-address: Address of the multicast group that the simulated host is to join, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Address of the multicast source that the simulated host is to join. The value of this argument should be a valid unicast address or 0.0.0.0. If the value is 0.0.0.0, this means that no multicast source is specified.

vlan *vlan-id*: Specifies the VLAN that comprises the port(s), where *vlan-id* is in the range of 1 to 4094.

Description

Use the **igmp-snooping host-join** command to configure the current port(s) as simulated member host(s), namely configure the current port as a member host for the specified multicast group or source and group.

Use the **undo igmp-snooping host-join** command to remove the current port(s) as simulated member host(s) for the specified multicast group or source and group.

By default, this function is disabled.

Note that:

- This command works on IGMP Snooping–enabled VLANs. The version of IGMP on the simulated host depends on the version of IGMP Snooping running in the VLAN.
- The **source-ip** *source-address* option in the command is meaningful only for IGMP Snooping version 3. If IGMP Snooping version 2 is running, although you can include **source-ip** *source-address* in the command, the simulated host does not respond to a query message.
- If configured in Ethernet port view or Layer 2 aggregate port view, this feature takes effect only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

Examples

Configure GIgabitEthernet1/0/1 as a simulated member host in VLAN 2 for multicast source 1.1.1.1 and multicast group 232.1.1.1.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping host-join 232.1.1.1 source-ip 1.1.1.1 vlan 2
```

igmp-snooping last-member-query-interval

Syntax

igmp-snooping last-member-query-interval *interval*

undo igmp-snooping last-member-query-interval

View

VLAN view

Default Level

2: System level

Parameters

interval: Interval between IGMP last-member queries, in seconds. The effective range is 1 to 5.

Description

Use the **igmp-snooping last-member-query-interval** command to configure the interval between IGMP last-member queries in the VLAN.

Use the **undo igmp-snooping last-member-query-interval** command to restore the default setting.

By default, the IGMP last-member query interval is 1 second.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **last-member-query-interval**.

Examples

Set the interval between IGMP last-member queries to 3 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping last-member-query-interval 3
```

igmp-snooping max-response-time

Syntax

igmp-snooping max-response-time *interval*

undo igmp-snooping max-response-time

View

VLAN view

Default Level

2: System level

Parameters

interval: Maximum response time to IGMP general queries, in seconds. The effective range is 1 to 25.

Description

Use the **igmp-snooping max-response-time** command to configure the maximum response time to IGMP general queries in the VLAN.

Use the **undo igmp-snooping max-response-time** command to restore the default setting.

By default, the maximum response time to IGMP general queries is 10 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **max-response-time**, **igmp-snooping query-interval**.

Examples

Set the maximum response time to IGMP general queries to 5 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping max-response-time 5
```

igmp-snooping overflow-replace

Syntax

igmp-snooping overflow-replace [**vlan** *vlan-list*]

undo igmp-snooping overflow-replace [**vlan** *vlan-list*]

View

Ethernet port view, Layer 2 aggregate port view, port group view

Default Level

2: System level

Parameters

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **igmp-snooping overflow-replace** command to enable the multicast group replacement function on the current port(s).

Use the **undo igmp-snooping overflow-replace** command to disable the multicast group replacement function on the current port(s).

By default, the multicast group replacement function is disabled.

Note that:

- This command works on IGMP Snooping–enabled VLANs.
- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).

Related commands: **overflow-replace**.

Examples

Enable the multicast group replacement function on GigabitEthernet1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping overflow-replace vlan 2
```

igmp-snooping querier

Syntax

igmp-snooping querier

undo igmp-snooping querier

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **igmp-snooping querier** command to enable the IGMP Snooping querier function.

Use the **undo igmp-snooping querier** command to disable the IGMP Snooping querier function.

By default, the IGMP Snooping querier function is disabled.

Note that:

- This command takes effect only if IGMP Snooping is enabled in the VLAN.
- This command does not take effect in a sub-VLAN of a multicast VLAN.

Related commands: **subvlan** in *Multicast VLAN Commands* in the *IP Multicast Volume*.

Examples

Enable the IGMP Snooping querier function in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping querier
```

igmp-snooping query-interval

Syntax

igmp-snooping query-interval *interval*

undo igmp-snooping query-interval

View

VLAN view

Default Level

2: System level

Parameters

interval: Interval between IGMP general queries, in seconds. The effective range is 2 to 300.

Description

Use the **igmp-snooping query-interval** command to configure the interval between IGMP general queries.

Use the **undo igmp-snooping query-interval** command to restore the default setting.

By default, the IGMP general query interval is 60 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **igmp-snooping querier**, **igmp-snooping max-response-time**, **max-response-time**.

Examples

Set the interval between IGMP general queries to 20 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping query-interval 20
```

igmp-snooping router-aging-time

Syntax

igmp-snooping router-aging-time *interval*

undo igmp-snooping router-aging-time

View

VLAN view

Default Level

2: System level

Parameters

interval: Dynamic router port aging time, in seconds. The effective range is 1 to 1,000.

Description

Use the **igmp-snooping router-aging-time** command to configure the aging time of dynamic router ports in the current VLAN.

Use the **undo igmp-snooping router-aging-time** command to restore the default setting.

By default, the aging time of dynamic router ports is 105 seconds.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Related commands: **router-aging-time**.

Examples

Set the aging time of dynamic router ports to 100 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping router-aging-time 100
```

igmp-snooping source-deny

Syntax

igmp-snooping source-deny

undo igmp-snooping source-deny

View

Ethernet port view, port group view

Default Level

2: System level

Parameters

None

Description

Use the **igmp-snooping source-deny** command to enable multicast source port filtering.

Use the **undo igmp-snooping source-deny** command to disable multicast source port filtering.

By default, multicast source port filtering is disabled.

This command works on IGMP Snooping–enabled VLANs.

Examples

Enable source port filtering for multicast data on GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping source-deny
```

igmp-snooping special-query source-ip

Syntax

igmp-snooping special-query source-ip { **current-interface** | *ip-address* }

undo igmp-snooping special-query source-ip

View

VLAN view

Default Level

2: System level

Parameters

current-interface: Sets the source address of IGMP group-specific queries to the address of the current VLAN interface. If the current VLAN interface does not have an IP address, the default IP address 0.0.0.0 will be used as the source IP address of IGMP group-specific queries.

ip-address: Sets the source address of IGMP group-specific queries to the specified address.

Description

Use the **igmp-snooping special-query source-ip** command to configure the source IP address of IGMP group-specific queries.

Use the **undo igmp-snooping special-query source-ip** command to restore the default configuration.

By default, the source IP address of IGMP group-specific queries is 0.0.0.0.

This command takes effect only if IGMP Snooping is enabled in the VLAN.

Examples

In VLAN 2 specify 10.1.1.1 as the source IP address of IGMP group-specific queries.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping special-query source-ip 10.1.1.1
```

igmp-snooping static-group

Syntax

igmp-snooping static-group *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping static-group *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

View

Ethernet port view, Layer 2 aggregate port view, port group view

Default Level

2: System level

Parameters

group-address: Address of the multicast group to be statically joined, in the range of 224.0.0.0 to 239.255.255.255.

source-address: Address of the multicast source to be statically joined. The value of this argument should be a valid unicast address or 0.0.0.0. If the value is 0.0.0.0, this means no multicast source is specified.

vlan *vlan-id*: Specifies the VLAN that comprises the port(s), where *vlan-id* is in the range of 1 to 4094.

Description

Use the **igmp-snooping static-group** command to configure the static (*, G) or (S, G) joining function, namely to configure the current port or port group as static multicast group or source-group member(s).

Use the **undo igmp-snooping static-group** command to restore the system default.

By default, no ports are static member ports.

Note that:

- The **source-ip** *source-address* option in the command is meaningful only for IGMP Snooping version 3. If IGMP Snooping version 2 is running, although you can include the **source-ip** *source-address* option in your command, the configuration will not take effect.
- If configured in Ethernet port view or Layer 2 aggregate port view, this feature takes effect only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

Examples

Configure GigabitEthernet1/0/1 in VLAN 2 to be a static member port for (1.1.1.1, 232.1.1.1).

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-group 232.1.1.1 source-ip 1.1.1.1 vlan
2
```

igmp-snooping static-router-port

Syntax

igmp-snooping static-router-port vlan *vlan-id*

undo igmp-snooping static-router-port vlan *vlan-id*

View

Ethernet port view, Layer 2 aggregate port view, port group view

Default Level

2: System level

Parameters

vlan *vlan-id*: Specifies a VLAN in which one or more static router ports are to be configured, where *vlan-id* is in the range of 1 to 4094.

Description

Use the **igmp-snooping static-router-port** command to configure the current port(s) as static router port(s).

Use the **undo igmp-snooping static-router-port** command to restore the system default.

By default, no ports are static router ports.

Note that:

- This command works on IGMP Snooping–enabled VLANs.
- This command does not take effect in a sub-VLAN of a multicast VLAN.
- If configured in Ethernet port view or Layer 2 aggregate port view, this feature takes effect only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

Related commands: **subvlan** in *Multicast VLAN Commands* in the *IP Multicast Volume*.

Examples

Enable the static router port function on GigabitEthernet1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-router-port vlan 2
```

igmp-snooping version

Syntax

igmp-snooping version *version-number*

undo igmp-snooping version

View

VLAN view

Default Level

2: System level

Parameters

version-number: IGMP snooping version, in the range of 2 to 3.

Description

Use the **igmp-snooping version** command to configure the IGMP Snooping version.

Use the **undo igmp-snooping version** command to restore the default setting.

By default, the IGMP Snooping version is 2.

Note that:

- This command can take effect only if IGMP Snooping is enabled in the VLAN.
- This command does not take effect in a sub-VLAN of a multicast VLAN.

Related commands: **igmp-snooping enable**; **subvlan** in *Multicast VLAN Commands* in the *IP Multicast Volume*.

Examples

Enable IGMP Snooping in VLAN 2, and set the IGMP Snooping version to version 3.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
```

last-member-query-interval (IGMP-Snooping view)

Syntax

last-member-query-interval *interval*

undo last-member-query-interval

View

IGMP-Snooping view

Default Level

2: System level

Parameters

interval: Interval between IGMP last-member queries, in seconds. The effective range is 1 to 5.

Description

Use the **last-member-query-interval** command to configure the interval between IGMP last-member queries globally.

Use the **undo last-member-query-interval** command to restore the default setting.

By default, the interval between IGMP last-member queries is 1 second.

This command works on IGMP Snooping–enabled VLANs.

Related commands: **igmp-snooping last-member-query-interval**.

Examples

Set the interval between IGMP last-member queries globally to 3 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] last-member-query-interval 3
```

max-response-time (IGMP-Snooping view)

Syntax

max-response-time *interval*

undo max-response-time

View

IGMP-Snooping view

Default Level

2: System level

Parameters

interval: Maximum response time to IGMP general queries, in seconds. The effective range is 1 to 25.

Description

Use the **max-response-time** command to configure the maximum response time to IGMP general queries globally.

Use the **undo max-response-time** command to restore the default value.

This command works on IGMP Snooping–enabled VLANs.

Related commands: **igmp-snooping max-response-time**, **igmp-snooping query-interval**.

Examples

Set the maximum response time to IGMP general queries globally to 5 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] max-response-time 5
```

overflow-replace (IGMP-Snooping view)

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

View

IGMP-Snooping view

Default Level

2: System level

Parameters

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **overflow-replace** command to enable the multicast group replacement function globally.

Use the **undo overflow-replace** command to disable the multicast group replacement function globally.

By default, the multicast group replacement function is disabled.

Note that:

- This command works on IGMP Snooping–enabled VLANs.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

Related commands: **igmp-snooping overflow-replace**.

Examples

Enable the multicast group replacement function globally in VLAN 2.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] overflow-replace vlan 2
```

report-aggregation (IGMP-Snooping view)

Syntax

report-aggregation

undo report-aggregation

View

IGMP-Snooping view

Default Level

2: System level

Parameters

None

Description

Use the **report-aggregation** command to enable IGMP report suppression.

Use the **undo report-aggregation** command to disable IGMP report suppression.

By default, IGMP report suppression is enabled.

This command works on IGMP Snooping–enabled VLANs.

Examples

Disable IGMP report suppression.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] undo report-aggregation
```

reset igmp-snooping group

Syntax

reset igmp-snooping group { *group-address* | **all** } [**vlan** *vlan-id*]

View

User view

Default Level

2: System level

Parameters

group-address: Clears the information about the specified multicast group. The value range of *group-address* is 224.0.1.0 to 239.255.255.255.

all: Clears all IGMP Snooping multicast group information.

vlan *vlan-id*: Clears the IGMP Snooping multicast group information in the specified VLAN. The effective range of *vlan-id* is 1 to 4094.

Description

Use the **reset igmp-snooping group** command to clear IGMP Snooping multicast group information.

Note that:

- This command works on IGMP Snooping–enabled VLANs.
- This command cannot clear IGMP Snooping multicast group information of static joins.

Examples

Clear all IGMP Snooping multicast group information.

```
<Sysname> reset igmp-snooping group all
```

reset igmp-snooping statistics

Syntax

reset igmp-snooping statistics

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **reset igmp-snooping statistics** command to clear the statistics information of IGMP messages learned by IGMP Snooping.

Examples

Clear the statistics information of all kinds of IGMP messages learned by IGMP Snooping.

```
<Sysname> reset igmp-snooping statistics
```

router-aging-time (IGMP-Snooping view)

Syntax

router-aging-time *interval*

undo router-aging-time

View

IGMP-Snooping view

Default Level

2: System level

Parameters

interval: Dynamic router port aging time, in seconds. The effective range is 1 to 1,000.

Description

Use the **router-aging-time** command to configure the aging time of dynamic router ports globally.

Use the **undo router-aging-time** command to restore the default setting.

By default, the aging time of dynamic router ports is 105 seconds.

This command works on IGMP Snooping–enabled VLANs.

Related commands: **igmp-snooping router-aging-time**.

Examples

Set the aging time of dynamic router ports globally to 100 seconds.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] router-aging-time 100
```

source-deny (IGMP-Snooping view)

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

View

IGMP-Snooping view

Default Level

2: System level

Parameters

interface-list: Specifies one or multiple ports. You can provide up to ten port lists, by each of which you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number* **to** *interface-type end-interface-number*, where the end interface number must be greater than the start interface number.

Description

Use the **source-deny** command to enable multicast source port filtering so that all multicast data packets are blocked.

Use the **undo source-deny** command to disable multicast source port filtering.

By default, multicast source port filtering is not enabled.

This command works on IGMP Snooping–enabled VLANs.

Examples

Enable source port filtering for multicast data on interfaces GigabitEthernet1/0/1 through GigabitEthernet1/0/4.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] source-deny port gigabitethernet1/0/1 to gigabitethernet1/0/4
```

2 Multicast VLAN Configuration Commands

Multicast VLAN Configuration Commands

display multicast-vlan

Syntax

display multicast-vlan [*vlan-id*]

View

Any view

Default Level

1: Monitor level

Parameters

vlan-id: VLAN ID of a multicast VLAN, in the range of 1 to 4094. If this argument is not provided, the information about all multicast VLANs will be displayed.

Description

Use the **display multicast-vlan** command to view the information about the specified multicast VLAN.

Examples

View the information about all multicast VLANs.

```
<Sysname> display multicast-vlan
 Total 1 multicast-vlan(s)

 Multicast vlan 100
   subvlan list:
    vlan 2  4-6
   port list:
    no port
```

Table 2-1 display multicast-vlan command output description

Field	Description
Total 1 multicast-vlan(s)	Total number of multicast VLANs
Multicast vlan	A multicast VLAN
subvlan list	List of sub-VLANs of the multicast VLAN
port list	Port list of the multicast VLAN

multicast-vlan

Syntax

multicast-vlan *vlan-id*

undo multicast-vlan { **all** | *vlan-id* }

View

System view

Default Level

2: System level

Parameters

vlan-id: Specifies a VLAN by its ID, in the range of 1 to 4094.

all: Deletes all multicast VLANs.

Description

Use the **multicast-vlan** command to configure the specified VLAN as a multicast VLAN and enter multicast VLAN view.

Use the **undo multicast-vlan** command to remove the specified VLAN as a multicast VLAN.

The VLAN to be configured is not a multicast VLAN by default.

Note that:

- The specified VLAN to be configured as a multicast VLAN must exist.
- For a sub-VLAN-based multicast VLAN, you need to enable IGMP Snooping only in the multicast VLAN; for a port-based multicast VLAN, you need to enable IGMP Snooping in both the multicast VLAN and all the user VLANs.

Related commands: **igmp-snooping enable** in the *IGMP Snooping Commands* in the *IP Multicast Volume*.

Examples

Enable IGMP Snooping in VLAN 100. Configure it as a multicast VLAN and enter multicast VLAN view.

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 100
[Sysname-vlan100] igmp-snooping enable
[Sysname-vlan100] quit
[Sysname] multicast-vlan 100
[Sysname-mvlan-100]
```

port (multicast VLAN view)

Syntax

port *interface-list*

undo port { **all** | *interface-list* }

View

Multicast VLAN view

Default Level

2: System level

Parameters

interface-list: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number* **to** *interface-type end-interface-number*, where the end interface number must be greater than the start interface number.

all: Deletes all the ports in the current multicast VLAN.

Description

Use the **port** command to assign the specified port(s) to the current multicast VLAN.

Use the **undo port** command to delete the specified port(s) or all ports from the current multicast VLAN.

By default, a multicast VLAN has no ports.

Note that:

- A port can belong to only one multicast VLAN.
- Only the following types of ports can be configured as multicast VLAN ports: Ethernet, or Layer 2 aggregate ports.

Examples

Assign ports GigabitEthernet1/0/1 through GigabitEthernet1/0/5 to multicast VLAN 100.

```
<Sysname> system-view
[Sysname] multicast-vlan 100
[Sysname-mvlan-100] port gigabitethernet1/0/1 to gigabitethernet1/0/5
```

port multicast-vlan

Syntax

port multicast-vlan *vlan-id*

undo port multicast-vlan

View

Ethernet port view, Layer 2 aggregate port view, port group view.

Default Level

2: System level

Parameters

vlan-id: VLAN ID of the multicast VLAN you want to assign the current port(s) to, in the range of 1 to 4094.

Description

Use the **port multicast-vlan** command to assign the current port(s) to the specified multicast VLAN.

Use the **undo port multicast-vlan** command to restore the system default.

By default, a port does not belong to any multicast VLAN.

Note that a port can belong to only one multicast VLAN.

Examples

Assign GigabitEthernet1/0/1 to multicast VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname- gigabitethernet1/0/1] port multicast-vlan 100
```

subvlan (multicast VLAN view)

Syntax

subvlan *vlan-list*

undo subvlan { **all** | *vlan-list* }

View

Multicast VLAN view

Default Level

2: System level

Parameters

vlan-list: Specifies a VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

all: Deletes all the sub-VLANs of the current multicast VLAN.

Description

Use the **subvlan** command to configure sub-VLAN(s) for the current multicast VLAN.

Use the **undo subvlan** command to remove the specified sub-VLAN(s) or all sub-VLANs from the current multicast VLAN.

A multicast VLAN has no sub-VLANs by default.

Note that:

- The VLANs to be configured as sub-VLANs of the multicast VLAN must exist and must not be multicast VLANs or sub-VLANs of another multicast VLAN.
- The number of sub-VLANs of the multicast VLAN must not exceed 63

Examples

Configure VLAN 10 through VLAN 15 as sub-VLANs of multicast VLAN 100.

```
<Sysname> system-view
[Sysname] multicast-vlan 100
```

```
[Sysname-mvlan-100] subvlan 10 to 15
```

3 MLD Snooping Configuration Commands

MLD Snooping Configuration Commands

display mld-snooping group

Syntax

display mld-snooping group [**vlan** *vlan-id*] [**slot** *slot-number*] [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

vlan *vlan-id*: Displays the MLD Snooping multicast group information in the specified VLAN, where *vlan-id* is in the range of 1 to 4094. If you do not specify a VLAN, this command will display the MLD Snooping multicast group information in all VLANs.

slot *slot-number*: Displays information about MLD Snooping multicast groups on the specified IRF member device. The *slot-number* argument is the member number of the device in the IRF, which you can display with the **display irf** command. The value range for the *slot-number* argument depends on the number of members and numbering conditions in the current IRF. If no IRF exists, the *slot-number* argument is the current device number.

verbose: Displays the detailed MLD Snooping multicast group information.

Description

Use the **display mld-snooping group** command to view the MLD Snooping multicast group information.

Examples

View the detailed MLD Snooping multicast group information in VLAN 2.

```
<Sysname> display mld-snooping group vlan 2 verbose
  Total 1 IP Group(s).
  Total 1 IP Source(s).
  Total 1 MAC Group(s).

  Port flags: D-Dynamic port, S-Static port, C-Copy port
  Subvlan flags: R-Real VLAN, C-Copy VLAN
  Vlan(id):2.
    Total 1 IP Group(s).
    Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
Router port(s):total 1 port.
       GE1/0/1             (D) ( 00:01:30 )
IP group(s):the following ip group(s) match to one mac group.
  IP group address:FF1E::101
    (::, FF1E::101):
      Attribute:    Host Port
      Host port(s):total 1 port.
        GE1/0/2             (D) ( 00:03:23 )
MAC group(s):
    MAC group address:3333-0000-0101
      Host port(s):total 1 port.
        GE1/0/2
```

Table 3-1 display mld-snooping group command output description

Field	Description
Total 1 IP Group(s).	Total number of IPv6 multicast groups
Total 1 IP Source(s).	Total number of IPv6 multicast sources
Total 1 MAC Group(s).	Total number of MAC multicast groups
Port flags: D-Dynamic port, S-Static port, C-Copy port	Port flags: D for dynamic port, S for static port, C for port copied from a (*, G) entry to an (S, G) entry
Subvlan flags: R-Real VLAN, C-Copy VLAN	Sub-VLAN flags: R for real egress sub-VLAN under the current entry, C for sub-VLAN copied from a (*, G) entry to an (S, G) entry
Router port(s)	Number of router ports
(00:01:30)	Remaining time of the dynamic member port or router port aging timer.
IP group address	Address of IPv6 multicast group
(::, FF1E::101)	(S, G) entry, :: represents all the multicast sources
MAC group address	Address of MAC multicast group
Attribute	Attribute of IPv6 multicast group
Host port(s)	Number of member ports

display mld-snooping statistics

Syntax

display mld-snooping statistics

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display mld-snooping statistics** command to view the statistics information of MLD messages learned by MLD Snooping.

Examples

View the statistics information of all kinds of MLD messages learned by MLD Snooping.

```
<Sysname> display mld-snooping statistics
  Received MLD general queries:0.
  Received MLDv1 specific queries:0.
  Received MLDv1 reports:0.
  Received MLD dones:0.
  Sent    MLDv1 specific queries:0.
  Received MLDv2 reports:0.
  Received MLDv2 reports with right and wrong records:0.
  Received MLDv2 specific queries:0.
  Received MLDv2 specific sg queries:0.
  Sent    MLDv2 specific queries:0.
  Sent    MLDv2 specific sg queries:0.
  Received error MLD messages:0.
```

Table 3-2 display mld-snooping statistics command output description

Field	Description
general queries	General query messages
specific queries	Multicast-address-specific query messages
reports	Report messages
dones	Done messages
reports with right and wrong records	Reports containing correct and incorrect records
specific sg queries	Multicast-address-and-source-specific queries
error MLD messages	Error MLD messages

fast-leave (MLD-Snooping view)

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

View

MLD-Snooping view

Default Level

2: System level

Parameters

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **fast-leave** command to enable fast leave processing globally. With this function enabled, when the switch receives an MLD leave message on a port, it directly removes that port from the forwarding table entry for the specific group.

Use the **undo fast-leave** command to disable fast leave processing globally.

By default, fast leave processing is disabled.

Note that:

- This command works on MLD Snooping–enabled VLANs.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

Related commands: **mld-snooping fast-leave**.

Examples

Enable fast leave processing globally in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] fast-leave vlan 2
```

group-policy (MLD-Snooping view)

Syntax

group-policy *acl6-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

View

MLD-Snooping view

Default Level

2: System level

Parameters

Acl6-number: Basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The source address or address range specified in the advanced IPv6 ACL rule is used to match the IPv6 multicast source address(es) specified in MLDv2 reports, rather than the source address in the IPv6 packets. The system assumes that an MLDv1 report or an MLDv2 IS_EX or TO_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **group-policy** command to configure a global IPv6 multicast group filter, namely to control the IPv6 multicast groups a host can join.

Use the **undo group-policy** command to remove the configured global IPv6 multicast group filter.

By default, no IPv6 multicast group filter is configured globally, namely any host can join any valid IPv6 multicast group.

Note that:

- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.
- If the specified IPv6 ACL does not exist or the ACL rule is null, all IPv6 multicast groups will be filtered out.
- You can configure different IPv6 ACL rules for each port in different VLANs; for a given VLAN, a newly configured IPv6 ACL rule will override the existing one.

Related commands: **mld-snooping group-policy**.

Examples

Apply ACL 2000 as an IPv6 multicast group filter in VLAN 2 so that hosts in this VLAN can join ff03::101 only.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff03::101 16
[Sysname-acl6-basic-2000] quit
[Sysname] mld-snooping
[Sysname-mld-snooping] group-policy 2000 vlan 2
```

host-aging-time (MLD-Snooping view)

Syntax

host-aging-time *interval*

undo host-aging-time

View

MLD-Snooping view

Default Level

2: System level

Parameters

interval: Dynamic member port aging time, in units of seconds. The effective range is 200 to 1,000.

Description

Use the **host-aging-time** command to configure the aging time of dynamic member ports globally.

Use the **undo host-aging-time** command to restore the default setting.

By default, the aging time of dynamic member ports is 260 seconds.

This command works on MLD Snooping–enabled VLANs

Related commands: **mld-snooping host-aging-time**.

Examples

Set the aging time of dynamic member ports globally to 300 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] host-aging-time 300
```

last-listener-query-interval (MLD-Snooping view)

Syntax

last-listener-query-interval *interval*

undo last-listener-query-interval

View

MLD-Snooping view

Default Level

2: System level

Parameters

interval: MLD last listener query interval in units of seconds, namely the length of time the device waits between sending MLD multicast-address-specific queries. The effective range is 1 to 5.

Description

Use the **last-listener-query-interval** command to configure the MLD last listener query interval globally.

Use the **undo last-listener-query-interval** command to restore the system default.

By default, the MLD last listener query interval is 1 second.

This command works on MLD Snooping–enabled VLANs.

Related commands: **mld-snooping last-listener-query-interval**.

Examples

Set the MLD last listener query interval to 3 seconds globally.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] last-listener-query-interval 3
```

max-response-time (MLD-Snooping view)

Syntax

max-response-time *interval*

undo max-response-time

View

MLD-Snooping view

Default Level

2: System level

Parameters

interval: Maximum response time for MLD general queries, in units of seconds. The effective range is 1 to 25.

Description

Use the **max-response-time** command to configure the maximum response time for MLD general queries globally.

Use the **undo max-response-time** command to restore the system default.

By default, the maximum response time for MLD general queries is 10 seconds.

This command works on MLD Snooping–enabled VLANs.

Related commands: **mld-snooping max-response-time**, **mld-snooping query-interval**.

Examples

Set the maximum response time for MLD general queries globally to 5 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] max-response-time 5
```

mld-snooping

Syntax

mld-snooping

undo mld-snooping

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **mld-snooping** command to enable MLD Snooping globally and enter MLD-Snooping view.

Use the **undo mld-snooping** command to disable MLD Snooping globally.

By default, MLD Snooping is disabled.

Related commands: **mld-snooping enable**.

Examples

Enable MLD Snooping globally and enter MLD-Snooping view.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping]
```

mld-snooping enable

Syntax

mld-snooping enable

undo mld-snooping enable

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **mld-snooping enable** command to enable MLD Snooping in the current VLAN.

Use the **undo mld-snooping enable** command to disable MLD Snooping in the current VLAN.

By default, MLD Snooping is disabled in a VLAN.

MLD Snooping must be enabled globally before it can be enabled in a VLAN

Related commands: **mld-snooping**.

Examples

Enable MLD Snooping in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
```

mld-snooping fast-leave

Syntax

mld-snooping fast-leave [**vlan** *vlan-list*]

undo mld-snooping fast-leave [**vlan** *vlan-list*]

View

Ethernet port view, Layer 2 aggregate port view, port group view

Default Level

2: System level

Parameters

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **mld-snooping fast-leave** command to enable fast leave processing on the current port or group of ports. With this function enabled, when the switch receives an MLD leave message on a port, it directly removes that port from the forwarding table entry for the specific group.

Use the **undo mld-snooping fast-leave** command to disable fast leave processing on the current port or group of ports.

By default, fast leave processing is disabled.

Note that:

- This command works on MLD Snooping–enabled VLANs.
- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).

Related commands: **fast-leave**.

Examples

Enable fast leave processing on GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping fast-leave vlan 2
```

mld-snooping general-query source-ip

Syntax

mld-snooping general-query source-ip { **current-interface** | *ipv6-address* }

undo mld-snooping general-query source-ip

View

VLAN view

Default Level

2: System level

Parameters

current-interface: Sets the source IPv6 link-local address of MLD general queries to the IPv6 address of the current VLAN interface. If the current VLAN interface does not have an IPv6 address, the default IPv6 address FE80::02FF:FFFF:FE00:0001 will be used as the source IPv6 address of MLD general queries.

ipv6-address: Specifies the source IPv6 address of MLD general queries, which can be any legal IPv6 link-local address.

Description

Use the **mld-snooping general-query source-ip** command to configure the source IPv6 address of MLD general queries.

Use the **undo mld-snooping general-query source-ip** command to restore the default configuration.

By default, the source IPv6 address of MLD general queries is FE80::02FF:FFFF:FE00:0001.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Examples

In VLAN 2, specify FE80:0:0:1::1 as the source IPv6 address of MLD general queries.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping general-query source-ip fe80:0:0:1::1
```

mld-snooping group-limit

Syntax

mld-snooping group-limit *limit* [**vlan** *vlan-list*]

undo mld-snooping group-limit [**vlan** *vlan-list*]

View

Ethernet port view, Layer 2 aggregate port view, port group view

Default Level

2: System level

Parameters

limit: Maximum number of IPv6 multicast groups that can be joined on a port. The value is in the range 1 to 1000.

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id*

to *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **mld-snooping group-limit** command to configure the maximum number of IPv6 multicast groups that can be joined on a port.

Use the **undo mld-snooping group-limit** command to restore the default setting.

By default, maximum number of IPv6 multicast groups that can be joined on a port is 1000.

Note that:

- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).

Examples

Specify to allow a maximum of 10 IPv6 multicast groups to be joined on GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] mld-snooping group-limit 10 vlan 2
```

mld-snooping group-policy

Syntax

mld-snooping group-policy *acl6-number* [**vlan** *vlan-list*]

undo mld-snooping group-policy [**vlan** *vlan-list*]

View

Ethernet port view, Layer 2 aggregate port view, port group view

Default Level

2: System level

Parameters

acl6-number: Basic or advanced IPv6 ACL number, in the range of 2000 to 3999. The IPv6 source address or address range specified in the advanced IPv6 ACL rule is the IPv6 multicast source address(es) specified in MLDv2 reports, rather than the source address in the IPv6 packets. The system assumes that an MLDv1 report or an MLDv2 IS_EX or TO_EX report that does not carry an IPv6 multicast source address carries an IPv6 multicast source address of 0::0.

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **mld-snooping group-policy** command to configure an IPv6 multicast group filter on the current port(s), namely to control the IPv6 multicast groups hosts on the port(s) can join.

Use the **undo mld-snooping group-policy** command to remove the configured IPv6 multicast group filter on the current port(s).

By default, no IPv6 multicast group filter is configured on a port, namely a host can join any valid IPv6 multicast group.

Note that:

- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).
- If the specified ACL does not exist or the ACL rule is null, all IPv6 multicast groups will be filtered out.
- You can configure different IPv6 ACL rules for each port in different VLANs; for a given VLAN, a newly configured IPv6 ACL rule will override the existing one.

Related commands: **group-policy**.

Examples

Apply ACL 2000 as an IPv6 multicast group filter so that hosts on GigabitEthernet 1/0/1 in VLAN 2 can join ff03::101 only.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff03::101 16
[Sysname-acl6-basic-2000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] mld-snooping group-policy 2000 vlan 2
```

mld-snooping host-aging-time

Syntax

mld-snooping host-aging-time *interval*

undo mld-snooping host-aging-time

View

VLAN view

Default Level

2: System level

Parameters

interval: Dynamic member port aging time, in seconds. The effective range is 200 to 1,000.

Description

Use the **mld-snooping host-aging-time** command to configure the aging time of dynamic member ports in the current VLAN.

Use the **undo mld-snooping host-aging-time** command to restore the system default.

By default, the dynamic member port aging time is 260 seconds.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **host-aging-time**.

Examples

Set the aging time of dynamic member ports to 300 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping host-aging-time 300
```

mld-snooping host-join

Syntax

mld-snooping host-join *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

undo mld-snooping host-join *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

View

Ethernet port view, Layer 2 aggregate port view, port group view

Default Level

2: System level

Parameters

ipv6-group-address: Address of IPv6 multicast group which the simulated host is to join. The effective range is FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where x and y represent any hexadecimal number between 0 and F, inclusive.

ipv6-source-address: Address of the IPv6 multicast source that the simulated host is to join.

vlan *vlan-id*: Specifies a VLAN that comprises the port(s), where *vlan-id* is in the range of 1 to 4094.

Description

Use the **mld-snooping host-join** command to configure the current port(s) as simulated member host(s), namely configure the current port as member host for the specified IPv6 multicast group or source and group.

Use the **undo mld-snooping host-join** command to remove the current port(s) as simulated member host(s) for the specified IPv6 multicast group or source and group.

By default, no ports are configured as static member ports for any IPv6 multicast group or source and group.

Note that:

- This command works on MLD Snooping–enabled VLANs, and the version of MLD on the simulated host depends on the version of MLD Snooping running in the VLAN.

- The **source-ip** *ipv6-source-address* option in the command is meaningful only for MLD Snooping version 2. If MLD Snooping version 1 is running, although you can include **source-ip** *ipv6-source-address* in your command, the simulated host responses with only an MLDv1 report when receiving a query message.
- If configured in Ethernet port view or Layer 2 aggregate port view, this feature takes effect only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

Examples

Configure GigabitEthernet 1/0/1 in VLAN 2 to join (2002::22, FF3E::101) as a simulated host.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] mld-snooping host-join ff3e::101 source-ip 2002::22 vlan 2
```

mld-snooping last-listener-query-interval

Syntax

mld-snooping last-listener-query-interval *interval*

undo mld-snooping last-listener-query-interval

View

VLAN view

Default Level

2: System level

Parameters

interval: MLD last listener query interval in units of seconds, namely the length of time the device waits between sending IGMP multicast-address-specific queries. The effective range is 1 to 5.

Description

Use the **mld-snooping last-listener-query-interval** command to configure the MLD last-listener query interval in the VLAN.

Use the **undo mld-snooping last-listener-query-interval** command to restore the system default.

By default, the MLD last listener query interval is 1 second.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **last-listener-query-interval**.

Examples

Set the MLD last-listener query interval to 3 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping last-listener-query-interval 3
```

mld-snooping max-response-time

Syntax

mld-snooping max-response-time *interval*

undo mld-snooping max-response-time

View

VLAN view

Default Level

2: System level

Parameters

interval: Maximum response time for MLD general queries, in units of seconds. The effective range is 1 to 25.

Description

Use the **mld-snooping max-response-time** command to configure the maximum response time for MLD general queries in the VLAN.

Use the **undo mld-snooping max-response-time** command to restore the default setting.

By default, the maximum response time for MLD general queries is 10 seconds.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **max-response-time**, **mld-snooping query-interval**.

Examples

Set the maximum response time for MLD general queries to 5 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping max-response-time 5
```

mld-snooping overflow-replace

Syntax

mld-snooping overflow-replace [**vlan** *vlan-list*]

undo mld-snooping overflow-replace [**vlan** *vlan-list*]

View

Ethernet port view, Layer 2 aggregate port view, port group view

Default Level

2: System level

Parameters

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **mld-snooping overflow-replace** command to enable the IPv6 multicast group replacement function on the current port(s).

Use the **undo mld-snooping overflow-replace** command to disable the IPv6 multicast group replacement function on the current port(s).

By default, the IPv6 multicast group replacement function is disabled.

Note that:

- This command works on MLD Snooping–enabled VLANs.
- If you do not specify any VLAN when using this command in Ethernet port view or Layer 2 aggregate port view, the command will take effect for all VLANs the port belongs to; if you specify a VLAN or multiple VLANs, the command will take effect only if the port belongs to the specified VLAN(s).
- If you do not specify any VLAN when using this command in port group view, the command will take effect on all the ports in this group; if you specify a VLAN or multiple VLANs, the command will take effect only on those ports in this group that belong to the specified VLAN(s).

Related commands: **overflow-replace**.

Examples

Enable the IPv6 multicast group replacement function on GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitgthernet 1/0/1
[Sysname- GigabitEthernet 1/0/1] mld-snooping overflow-replace vlan 2
```

mld-snooping querier

Syntax

mld-snooping querier

undo mld-snooping querier

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **mld-snooping querier** command to enable the MLD Snooping querier function.

Use the **undo mld-snooping querier** command to disable the MLD Snooping querier function.

By default, the MLD Snooping querier function is disabled.

Note that:

- This command takes effect only if MLD Snooping is enabled in the VLAN.
- This command does not take effect in a sub-VLAN of an IPv6 multicast VLAN.

Related commands: **subvlan** command in *IPv6 Multicast VLAN Commands* in the *IP Multicast Volume*.

Examples

Enable the MLD Snooping querier function in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping querier
```

mld-snooping query-interval

Syntax

mld-snooping query-interval *interval*

undo mld-snooping query-interval

View

VLAN view

Default Level

2: System level

Parameters

interval: MLD query interval in seconds, namely the length of time the device waits between sending MLD general queries. The effective range is 2 to 300.

Description

Use the **mld-snooping query-interval** command to configure the MLD query interval.

Use the **undo mld-snooping query-interval** command to restore the system default.

By default, the MLD query interval is 125 seconds.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **mld-snooping querier**, **mld-snooping max-response-time**, **max-response-time**.

Examples

Set the MLD query interval to 20 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping query-interval 20
```

mld-snooping router-aging-time

Syntax

mld-snooping router-aging-time *interval*

undo mld-snooping router-aging-time

View

VLAN view

Default Level

2: System level

Parameters

interval: Dynamic router port aging time, in seconds. The effective range is 1 to 1,000.

Description

Use the **mld-snooping router-aging-time** command to configure the aging time of dynamic router ports in the current VLAN.

Use the **undo mld-snooping router-aging-time** command to restore the default setting.

By default, the dynamic router port aging time is 260 seconds.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Related commands: **router-aging-time**.

Examples

Set the aging time of dynamic router ports to 100 seconds in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping router-aging-time 100
```

mld-snooping source-deny

Syntax

mld-snooping source-deny

undo mld-snooping source-deny

View

Ethernet port view, port group view

Default Level

2: System level

Parameters

None

Description

Use the **mld-snooping source-deny** command to enable IPv6 multicast source port filtering.

Use the **undo mld-snooping source-deny** command to disable IPv6 multicast source port filtering.

By default, IPv6 multicast source port filtering is disabled.

Examples

Enable source port filtering for IPv6 multicast data on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] mld-snooping source-deny
```

mld-snooping special-query source-ip

Syntax

mld-snooping special-query source-ip { **current-interface** | *ipv6-address* }

undo mld-snooping special-query source-ip

View

VLAN view

Default Level

2: System level

Parameters

current-interface: Specifies the source IPv6 link-local address of the VLAN interface of the current VLAN as the source IPv6 address of MLD multicast-address-specific queries. If the current VLAN interface does not have an IPv6 address, the default IPv6 address FE80::02FF:FFFF:FE00:0001 will be used as the source IPv6 address of MLD multicast-address-specific queries.

ipv6-address: Specifies an IPv6 link-local address as the source IPv6 address of MLD multicast-address-specific queries.

Description

Use the **mld-snooping special-query source-ip** command to configure the source IPv6 address of MLD multicast-address-specific queries.

Use the **undo mld-snooping special-query source-ip** command to restore the default configuration.

By default, the source IPv6 address of MLD multicast-address-specific queries is FE80::02FF:FFFF:FE00:0001.

This command takes effect only if MLD Snooping is enabled in the VLAN.

Examples

In VLAN 2, specify FE80:0:0:1::1 as the source IPv6 address of MLD multicast-address-specific queries.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping special-query source-ip fe80:0:0:1::1
```

mld-snooping static-group

Syntax

mld-snooping static-group *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

undo mld-snooping static-group *ipv6-group-address* [**source-ip** *ipv6-source-address*] **vlan** *vlan-id*

View

Ethernet port view, Layer 2 aggregate port view, port group view

Default Level

2: System level

Parameters

ipv6-group-address: Address of a IPv6 multicast group the port(s) will be configured to join as static member port(s). The effective range is FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where x and y represent any hexadecimal number between 0 and F, inclusive.

ipv6-source-address: Address of the IPv6 multicast source the port(s) will be configured to join as static member port(s).

vlan *vlan-id*: Specifies the VLAN that comprises the Ethernet port(s), where *vlan-id* is in the range of 1 to 4094.

Description

Use the **mld-snooping static-group** command to configure the static IPv6 (*, G) or (S, G) joining function, namely to configure the port or port group as static IPv6 multicast group or source-group member(s).

Use the **undo mld-snooping static-group** command to restore the system default.

By default, no ports are static member ports.

Note that:

- The **source-ip** *ipv6-source-address* option in the command is meaningful only for MLD Snooping version 2. If MLD Snooping version 1 is running, although you can include **source-ip** *ipv6-source-address* in your command, the simulated host responses with only an MLDv1 report when receiving a query message.
- If configured in Ethernet port view or Layer 2 aggregate port view, this feature takes effect only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

Examples

Configure GigabitEthernet 1/0/1 in VLAN 2 to be a static member port for (2002::22, FF3E::101).

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname- GigabitEthernet 1/0/1] mld-snooping static-group ff3e::101 source-ip 2002::22 vlan
2
```

mld-snooping static-router-port

Syntax

mld-snooping static-router-port vlan *vlan-id*

undo mld-snooping static-router-port vlan *vlan-id*

View

Ethernet port view, Layer 2 aggregate port view, port group view

Default Level

2: System level

Parameters

vlan *vlan-id*: Specifies a VLAN in which one or more static router ports are to be configured, where *vlan-id* is in the range of 1 to 4094.

Description

Use the **mld-snooping static-router-port** command to configure the current port(s) as static router port(s).

Use the **undo mld-snooping static-router-port** command to restore the system default.

By default, no ports are static router ports.

Note that:

- This command works on MLD Snooping–enabled VLANs.
- This command does not take effect in a sub-VLAN of an IPv6 multicast VLAN.
- If configured in Ethernet port view or Layer 2 aggregate port view, this feature takes effect only if the port belongs to the specified VLAN.
- If configured in port group view, this feature takes effect only on those ports in this port group that belong to the specified VLAN.

Related commands: **subvlan** command in *IPv6 Multicast VLAN Commands* in the *IP Multicast Volume*.

Examples

Enable the static router port function on GigabitEthernet 1/0/1 in VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname- GigabitEthernet 1/0/1] mld-snooping static-router-port vlan 2
```

mld-snooping version

Syntax

mld-snooping version *version-number*

undo mld-snooping version

View

VLAN view

Default Level

2: System level

Parameters

version-number: MLD snooping version, in the range of 1 to 2.

Description

Use the **mld-snooping version** command to configure the MLD Snooping version.

Use the **undo mld-snooping version** command to restore the default setting.

By default, the MLD version is 1.

Note that:

- This command can take effect only if MLD Snooping is enabled in the VLAN.
- This command does not take effect in a sub-VLAN of an IPv6 multicast VLAN.

Related commands: **mld-snooping enable**; **subvlan** in *IPv6 Multicast VLAN Commands* in the *IP Multicast Volume*.

Examples

Enable MLD Snooping in VLAN 2, and set the MLD Snooping version to version 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping version 2
```

overflow-replace (MLD-Snooping view)

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

View

MLD-Snooping view

Default Level

2: System level

Parameters

vlan *vlan-list*: Defines one or multiple VLANs. You can provide up to 10 VLAN lists, by each of which you can specify an individual VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

Description

Use the **overflow-replace** command to enable the IPv6 multicast group replacement function globally.

Use the **undo overflow-replace** command to disable the IPv6 multicast group replacement function globally.

By default, the IPv6 multicast group replacement function is disabled globally.

Note that:

- This command works on MLD Snooping–enabled VLANs.
- If you do not specify any VLAN, the command will take effect for all VLANs; if you specify a VLAN or multiple VLANs, the command will take effect for the specified VLAN(s) only.

Related commands: **mld-snooping overflow-replace**.

Examples

Enable the IPv6 multicast group replacement function globally in VLAN 2.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] overflow-replace vlan 2
```

report-aggregation (MLD-Snooping view)

Syntax

report-aggregation

undo report-aggregation

View

MLD-Snooping view

Default Level

2: System level

Parameters

None

Description

Use the **mld-snooping report-aggregation** command to enable MLD report suppression.

Use the **undo mld-snooping report-aggregation** command to disable MLD report suppression.

By default, MLD report suppression is enabled.

This command works on MLD Snooping–enabled VLANs.

Examples

Disable MLD report suppression.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] undo report-aggregation
```

reset mld-snooping group

Syntax

reset mld-snooping group { *ipv6-group-address* | **all** } [**vlan** *vlan-id*]

View

User view

Default Level

2: System level

Parameters

ipv6-group-address: Clears the information about the specified multicast group. The effective range of *ipv6-group-address* is FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where x and y represent any hexadecimal number between 0 and F, inclusive.

all: Clears all MLD Snooping multicast group information.

vlan *vlan-id*: Clears the MLD Snooping multicast group information in the specified VLAN. The effective range of *vlan-id* is 1 to 4094.

Description

Use the **reset mld-snooping group** command to clear MLD Snooping multicast group information.

Note that:

- This command works on MLD Snooping–enabled VLANs.
- This command cannot clear MLD Snooping multicast group information of static joining.

Examples

Clear all MLD Snooping multicast group information.

```
<Sysname> reset mld-snooping group all
```

reset mld-snooping statistics

Syntax

reset mld-snooping statistics

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **reset mld-snooping statistics** command to clear the statistics information of MLD messages learned by MLD Snooping.

Examples

Clear the statistics information of all kinds of MLD messages learned by MLD Snooping.

```
<Sysname> reset mld-snooping statistics
```

router-aging-time (MLD-Snooping view)

Syntax

router-aging-time *interval*

undo router-aging-time

View

MLD-Snooping view

Default Level

2: System level

Parameters

interval: Dynamic router port aging time, in seconds. The effective range is 1 to 1,000.

Description

Use the **router-aging-time** command to configure the aging time of dynamic router ports globally.

Use the **undo router-aging-time** command to restore the default setting.

By default, the dynamic router port aging time is 260 seconds.

This command works on MLD Snooping–enabled VLANs.

Related commands: **mld-snooping router-aging-time**.

Examples

Set the aging time of dynamic router ports globally to 100 seconds.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] router-aging-time 100
```

source-deny (MLD-Snooping view)

Syntax

source-deny port *interface-list*

undo source-deny port *interface-list*

View

MLD-Snooping view

Default Level

2: System level

Parameters

interface-list: Port list. You can specify multiple ports or port ranges by providing the this argument in the form of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] }, where *interface-type* is port type and *interface-number* is port number.

Description

Use the **source-deny** command to enable IPv6 multicast source port filtering, namely to filter out all the received IPv6 multicast packets.

Use the **undo source-deny** command to disable IPv6 multicast source port filtering.

By default, IPv6 multicast source port filtering is disabled.

This command works on MLD Snooping–enabled VLANs.

Examples

Enable source port filtering for IPv6 multicast data on interfaces GigabitEthernet1/0/1 through GigabitEthernet1/0/4.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] source-deny port gigabitethernet1/0/1 to gigabitethernet1/0/4
```

4 IPv6 Multicast VLAN Configuration Commands

IPv6 Multicast VLAN Configuration Commands

display multicast-vlan ipv6

Syntax

display multicast-vlan ipv6 [*vlan-id*]

View

Any view

Default Level

1: Monitor level

Parameters

vlan-id: VLAN ID of an IPv6 multicast VLAN, in the range of 1 to 4094. If this argument is not provided, the information about all IPv6 multicast VLANs will be displayed.

Description

Use the **display multicast-vlan ipv6** command to view the information about the specified IPv6 multicast VLAN or all IPv6 multicast VLANs.

Examples

View the information about all IPv6 multicast VLANs.

```
<Sysname> display multicast-vlan ipv6
 Total 1 IPv6 multicast-vlan(s)
 IPv6 Multicast vlan 100
   subvlan list:
    vlan 2  4-6
   port list:
    no port
```

Table 4-1 display multicast-vlan ipv6 command output description

Field	Description
Total 1 IPv6 multicast-vlan(s)	Total number of IPv6 multicast VLANs
IPv6 Multicast vlan	An IPv6 multicast VLAN
subvlan list	List of sub-VLANs of the IPv6 multicast VLAN
port list	Port list of the IPv6 multicast VLAN

multicast-vlan ipv6

Syntax

multicast-vlan ipv6 *vlan-id*

undo multicast-vlan ipv6 { **all** | *vlan-id* }

View

System view

Default Level

2: System level

Parameters

vlan-id: Specifies a VLAN by its ID, in the range of 1 to 4094.

all: Deletes all IPv6 multicast VLANs.

Description

Use the **multicast-vlan ipv6** command to configure the specified VLAN as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.

Use the **undo multicast-vlan ipv6** command to remove the specified VLAN as an IPv6 multicast VLAN.

No VLAN is an IPv6 multicast VLAN by default.

Note that:

- The specified VLAN to be configured as an IPv6 multicast VLAN must exist.
- For a sub-VLAN-based IPv6 multicast VLAN, you need to enable MLD Snooping only in the IPv6 multicast VLAN; for a port-based IPv6 multicast VLAN, you need to enable MLD Snooping in both the IPv6 multicast VLAN and all the user VLANs.

Related commands: **mld-snooping enable** in the *MLD Snooping Commands* in the *IP Multicast Volume*.

Examples

Enable MLD Snooping in VLAN 100. Configure it as an IPv6 multicast VLAN and enter IPv6 multicast VLAN view.

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 100
[Sysname-vlan100] mld-snooping enable
[Sysname-vlan100] quit
[Sysname] multicast-vlan ipv6 100
[Sysname-ipv6-mvlan-100]
```

port (IPv6 multicast VLAN view)

Syntax

port *interface-list*

undo port { **all** | *interface-list* }

View

IPv6 multicast VLAN view

Default Level

2: System level

Parameters

interface-list: Specifies a port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number* **to** *interface-type end-interface-number*, where the end interface number must be greater than the start interface number.

all: Deletes all the ports in the current IPv6 multicast VLAN.

Description

Use the **port** command to assign port(s) to the current IPv6 multicast VLAN.

Use the **undo port** command to delete port(s) from the current IPv6 multicast VLAN.

By default, an IPv6 multicast VLAN has no ports.

Note that:

- A port can belong to only one IPv6 multicast VLAN.
- Only the following types of ports can be configured as IPv6 multicast VLAN ports: Ethernet, and Layer 2 aggregate ports.

Examples

Assign ports GigabitEthernet1/0/1 through GigabitEthernet1/0/5 to IPv6 multicast VLAN 100.

```
<Sysname> system-view
[Sysname] multicast-vlan ipv6 100
[Sysname-ipv6-mvlan-100] port gigabitethernet1/0/1 to gigabitethernet1/0/5
```

port multicast-vlan ipv6

Syntax

port multicast-vlan ipv6 *vlan-id*

undo port multicast-vlan ipv6

View

Ethernet port view, Layer 2 aggregate port view, port group view.

Default Level

2: System level

Parameters

vlan-id: VLAN ID of the IPv6 multicast VLAN you want to assign the current port(s) to, in the range of 1 to 4094.

Description

Use the **port multicast-vlan ipv6** command to assign the current port(s) to the specified IPv6 multicast VLAN.

Use the **undo port multicast-vlan ipv6** command to restore the system default.

By default, a port does not belong to any IPv6 multicast VLAN.

Note that a port can belong to only one IPv6 multicast VLAN.

Examples

Assign GigabitEthernet1/0/1 to IPv6 multicast VLAN 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname- GigabitEthernet1/0/1] port multicast-vlan ipv6 100
```

subvlan (IPv6 multicast VLAN view)

Syntax

subvlan *vlan-list*

undo subvlan { **all** | *vlan-list* }

View

IPv6 multicast VLAN view

Default Level

2: System level

Parameters

vlan-list: Specifies a VLAN in the form of *vlan-id*, or a VLAN range in the form of *start-vlan-id* **to** *end-vlan-id*, where the end VLAN ID must be greater than the start VLAN ID. The effective range of a VLAN ID is 1 to 4094.

all: Deletes all the sub-VLANs of the current IPv6 multicast VLAN.

Description

Use the **subvlan** command to configure sub-VLAN(s) for the current IPv6 multicast VLAN.

Use the **undo subvlan** command to remove the specified sub-VLAN(s) or all sub-VLANs from the current IPv6 multicast VLAN.

An IPv6 multicast VLAN has no sub-VLANs by default.

Note that:

- The VLANs to be configured as the sub-VLANs of the IPv6 multicast VLAN must exist and must not be IPv6 multicast VLANs or sub-VLANs of another IPv6 multicast VLAN.
- The number of sub-VLANs of the multicast VLAN must not exceed 63.

Examples

Configure VLAN 10 through VLAN 15 as sub-VLANs of IPv6 multicast VLAN 100.

```
<Sysname> system-view
[Sysname] multicast-vlan ipv6 100
[Sysname-ipv6-mvlan-100] subvlan 10 to 15
```

Table of Contents

1 QoS Policy Configuration Commands

Commands for Defining Classes

display traffic classifier

Syntax

display traffic classifier user-defined [*classifier-name*]

View

Any view

Default Level

1: Monitor level

Parameters

classifier-name: Class name.

Description

Use the **display traffic classifier** command to display the information about a class.

If no class name is provided, this command displays the information about all the user-defined classes.

Examples

Display the information about the user-defined classes.

```
<Sysname> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: p
    Operator: AND
    Rule(s) : If-match acl 2001
```

Table 1-1 display traffic classifier user-defined command output description

Field	Description
User Defined Classifier Information	The information about the user-defined classes is displayed.
Classifier	Class name and its contents, which could be of multiple types
Operator	Logical relationship among the classification rules
Rule	Classification rules

if-match

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

View

Class view

Default Level

2: System Level

Parameters

match-criteria: Matching rule to be defined. Table 1-2 describes the available forms of this argument.

Table 1-2 The forms of the *match-criteria* argument

Field	Description
acl *access-list-number*	Specifies an ACL to match packets. The *access-list-number* argument is a number in the range 2000 to 4999 or an ACL name. In a class configured with the operator **and**, the logical relationship between rules defined in the referenced IPv4 ACL is **or**.
acl ipv6 *access-list-number*	Specifies an IPv6 ACL to match IPv6 packets. The *access-list-number* argument is a number in the range 2000 to 3999 or an ACL name. In a class configured with the operator **and**, the logical relationship between rules defined in the referenced IPv6 ACL is **or**.
any	Specifies to match all packets.
customer-dot1p *8021p-list*	Specifies to match packets by 802.1p precedence of the customer network. The *8021p-list* argument is a list of CoS values, in the range of 0 to 7. **Note** *Even though you can provide up to eight space-separated CoS values for this argument, the Switch 4210G series switches support only one CoS value in a rule. If you configure multiple CoS values in a rule, the rule cannot be issued.*
customer-vlan-id *vlan-id-list*	Specifies to match the packets of specified VLANs of user networks. The *vlan-id-list* argument specifies a list of VLAN IDs, in the form of *vlan-id* **to** *vlan-id* or multiple discontinuous VLAN IDs (separated by space). You can specify up to eight VLAN IDs for this argument at a time. VLAN ID is in the range 1 to 4094. In a class configured with the operator **and**, the logical relationship between the customer VLAN IDs specified for the **customer-vlan-id** keyword is **or**.

Field	Description
dscp *dscp-list*	Specifies to match packets by DSCP precedence. The *dscp-list* argument is a list of DSCP values in the range of 0 to 63 or keywords shown in Table 1-4.  **Note** *Even though you can provide up to eight space-separated DSCP values for this argument, the Switch 4210G series switches support only one DSCP value in a rule. If you configure multiple DSCP values in a rule, the rule cannot be issued.*
destination-mac *mac-address*	Specifies to match the packets with a specified destination MAC address.
ip-precedence *ip-precedence-list*	Specifies to match packets by IP precedence. The *ip-precedence-list* argument is a list of IP precedence values in the range of 0 to 7.  **Note** *Even though you can provide up to eight space-separated IP precedence values for this argument, the Switch 4210G series switches support only one IP precedence value in a rule. If you configure multiple IP precedence values in a rule, the rule cannot be issued.*
protocol *protocol-name*	Specifies to match the packets of a specified protocol. The *protocol-name* argument can be IP or IPv6.
service-dot1p *8021p-list*	Specifies to match packets by 802.1p precedence of the service provider network. The *8021p-list* argument is a list of CoS values in the range of 0 to 7.  **Note** *Even though you can provide up to eight space-separated CoS values for this argument, the Switch 4210G series switches support only one CoS value in a rule. If you configure multiple CoS values in a rule, the rule cannot be issued.*
service-vlan-id *vlan-id-list*	Specifies to match the packets of specified VLANs of the operator's network. The *vlan-id-list* argument is a list of VLAN IDs, in the form of *vlan-id* **to** *vlan-id* or multiple discontinuous VLAN IDs (separated by space). You can specify up to eight VLAN IDs for this argument at a time. VLAN ID is in the range 1 to 4094. In a class configured with the operator **and**, the logical relationship between the service VLAN IDs specified for the **service-vlan-id** keyword is **or**.
source-mac *mac-address*	Specifies to match the packets with a specified source MAC address.

Description

Use the **if-match** command to define a rule to match a specific type of packets.

Use the **undo if-match** command to remove a matching rule.

Note

Suppose the logical relationship between classification rules is **and**. Note the following when using the **if-match** command to define matching rules.

- If multiple matching rules with the **acl** or **acl ipv6** keyword specified are defined in a class, the actual logical relationship between these rules is **or** when the policy is applied.
- If multiple matching rules with the **customer-vlan-id** or **service-vlan-id** keyword specified are defined in a class, the actual logical relationship between these rules is **or** when the policy is applied.

Examples

Define a rule for class1 to match the packets with their destination MAC addresses being 0050-ba27-bed3.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match destination-mac 0050-ba27-bed3
```

Define a rule for class2 to match the packets with their source MAC addresses being 0050-ba27-bed2.

```
<Sysname> system-view
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match source-mac 0050-ba27-bed2
```

Define a rule for class3 to match the advanced IPv4 ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class3
[Sysname-classifier-class3] if-match acl 3101
```

Define a rule for class4 to match the advanced IPv6 ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class4
[Sysname-classifier-class4] if-match acl ipv6 3101
```

Define a rule for class5 to match all the packets.

```
<Sysname> system-view
[Sysname] traffic classifier class5
[Sysname-classifier-class5] if-match any
```

Define a rule for class6 to match the packets with their DSCP precedence values being 1.

```
<Sysname> system-view
[Sysname] traffic classifier class6
[Sysname-classifier-class6] if-match dscp 1
```

Define a rule for class7 to match the packets with their IP precedence values being 1.

```
<Sysname> system-view
[Sysname] traffic classifier class7
[Sysname-classifier-class7] if-match ip-precedence 1
```

Define a rule for class8 to match IP packets.

```
<Sysname> system-view
[Sysname] traffic classifier class8
[Sysname-classifier-class8] if-match protocol ip
```

Define a rule for class9 to match the packets with the customer network 802.1p precedence 2.

```
<Sysname> system-view
[Sysname] traffic classifier class9
[Sysname-classifier-class9] if-match customer-dot1p 2
```

Define a rule for class10 to match the packets with the service provider network 802.1p precedence 5.

```
<Sysname> system-view
[Sysname] traffic classifier class10
[Sysname-classifier-class10] if-match service-dot1p 5
```

Define a rule for class11 to match the packets of customer VLAN 1024.

```
<Sysname> system-view
[Sysname] traffic classifier class11
[Sysname-classifier-class11] if-match customer-vlan-id 1024
```

Define a rule for class12 to match the packets of service VLAN 1000.

```
<Sysname> system-view
[Sysname] traffic classifier class12
[Sysname-classifier-class12] if-match service-vlan-id 1000
```

traffic classifier

Syntax

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

undo traffic classifier *classifier-name*

View

System view

Default Level

2: System Level

Parameters

and: Specifies the relationship among the rules in the class as logic AND. That is, a packet is matched only when it matches all the rules defined for the class.

or: Specifies the relationship among the rules in the class as logic OR. That is, a packet is matched if it matches a rule defined for the class.

classifier-name: Name of the class to be created.

Description

Use the **traffic classifier** command to create a class. This command also leads you to class view.

Use the **undo traffic classifier** command to remove a class.

By default, a packet is matched only when it matches all the rules configured for the class.

Examples

Create a class named class 1.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1]
```

Traffic Behavior Configuration Commands

accounting

Syntax

accounting

undo accounting

View

Traffic behavior view

Default Level

2: System Level

Parameters

None

Description

Use the **accounting** command to configure the traffic accounting action for a traffic behavior.

Use the **undo accounting** command to remove the traffic accounting action.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples

Configure the traffic accounting action for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] accounting
```

car

Syntax

car cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**green** *action*] [**red** *action*] [**yellow** *action*]

undo car

View

Traffic behavior view

Default Level

2: System Level

Parameters

cir *committed-information-rate*: Specifies the committed information rate (CIR) in kbps. The *committed-information-rate* argument ranges from 64 to 32000000 and must be a multiple of 64.

cbs *committed-burst-size*: Specifies the committed burst size (CBS) in bytes. The *committed-burst-size* argument ranges from 4000 to 16000000, the default is 4000.

ebs *excess-burst-size*: Specifies excess burst size (EBS) in bytes. The *excess-burst-size* argument ranges from 0 to 16000000, the default is 4000.

pir *peak-information-rate*: Specifies the peak information rate (PIR) in kbps. The *peak-information-rate* argument ranges from 64 to 32000000 and must be a multiple of 64.

green *action*: Specifies the action to be conducted for the traffic conforming to CIR. The *action* argument can be:

- **discard**: Drops the packets.
- **pass**: Forwards the packets.
- **remark-dscp-pass** *new-dscp*: Marks the packets with a new DSCP precedence and forwards them to their destinations. The *new-dscp* argument is in the range 0 to 63.

By default, packets conforming to CIR are forwarded.

red *action*: Specifies the action to be conducted for the traffic conforms to neither CIR nor PIR. The *action* argument can be:

- **discard**: Drops the packets.
- **pass**: Forwards the packets.
- **remark-dscp-pass** *new-dscp*: Marks the packets with a new DSCP precedence and forwards them to their destinations. The *new-dscp* argument is in the range 0 to 63.

By default, packets conforming to neither CIR nor PIR are dropped.

yellow *action*: Specifies the action to be conducted for the traffic conforms to PIR but does not conform to CIR. The *action* argument can be:

- **discard**: Drops the packets.
- **pass**: Forwards the packets.
- **remark-dscp-pass** *new-dscp*: Marks the packets with a new DSCP precedence and forwards them to their destinations. The *new-dscp* argument is in the range 0 to 63.

By default, packets conforming to PIR but not conforming to CIR are forwarded.

Description

Use the **car** command to configure TP action for a traffic behavior.

Use the **undo car** command to remove the TP action.

Note that, if you configure the TP action for a traffic behavior for multiple times, only the last configuration takes effect.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples

Configure TP action for a traffic behavior. When the traffic rate is lower than 6400 kbps, packets are forwarded normally. When the traffic rate exceeds 6400 kbps, the packets beyond 6400 kbps are dropped.

```
<Sysname> system-view
```

```
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 6400 red discard
```

display traffic behavior

Syntax

display traffic behavior user-defined [*behavior-name*]

View

Any view

Default Level

1: Monitor level

Parameters

behavior-name: Name of a user defined traffic behavior.

Description

Use the **display traffic behavior** command to display the information about a user defined traffic behavior.

If no behavior name is provided, this command displays the information about all the user-defined behaviors.

Examples

Display the information about all the user defined traffic behaviors.

```
<Sysname> display traffic behavior user-defined
  User Defined Behavior Information:
    Behavior: test
      Marking:
        Remark dot1p COS 4
      Committed Access Rate:
        CIR 64 (kbps), CBS 4000 (byte), EBS 4000 (byte), PIR 640 (kbps)
        Green Action: pass
        Red Action: discard
        Yellow Action: pass
```

Table 1-3 display traffic behavior user-defined command output description

Field	Description
User Defined Behavior Information	The information about user defined traffic behaviors is displayed
Behavior	Name of a traffic behavior, which can be of multiple types
Marking	Information about priority marking
Committed Access Rate	Information about traffic rate limit
CIR	Committed information rate in bytes
CBS	Committed burst size in bytes

Field	Description
EBS	Excessive burst size in bytes
PIR	Peak information rate in bytes
Green Action	Action conducted to packets conforming to CIR
Red Action	Action conducted for packets conforming to neither CIR nor PIR
Yellow Action	Action conducted to packets conforming to PIR but not conforming to CIR

filter

Syntax

filter { **deny** | **permit** }

undo filter

View

Traffic behavior view

Default Level

2: System Level

Parameters

deny: Drops packets.

permit: Forwards packets.

Description

Use the **filter** command to configure traffic filtering action for a traffic behavior.

Use the **undo filter** command to remove the traffic filtering action.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples

Configure traffic filtering action for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] filter deny
```

redirect

Syntax

redirect { **cpu** | **interface** *interface-type interface-number* }

undo redirect { **cpu** | **interface** *interface-type interface-number* }

View

Traffic behavior view

Default Level

2: System Level

Parameters

cpu: Redirects traffic to the CPU.

interface *interface-type interface-number*: Redirects traffic to an interface identified by its type and number.

Description

Use the **redirect** command to configure traffic redirecting action for a traffic behavior.

Use the **undo redirect** command to remove the traffic redirecting action.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples

Configure the redirecting action to redirect traffic to GigabitEthernet 1/0/1 port.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface GigabitEthernet 1/0/1
```

remark dot1p

Syntax

remark dot1p *8021p*

undo remark dot1p

View

Traffic behavior view

Default Level

2: System Level

Parameters

8021p: 802.1p precedence to be set for packets, in the range 0 to 7.

Description

Use the **remark dot1p** command to configure the action of setting 802.1p precedence for a traffic behavior.

Use the **undo remark dot1p** command to remove the action of setting 802.1p precedence

Note that, when the **remark dot1p** command is used together with the **remark local-precedence** command, the 802.1p precedence to be set for packets must be the same as the local precedence to be set for packets. Otherwise, the corresponding policy cannot be applied successfully.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples

Configure the action to set 802.1p precedence to 2 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p 2
```

remark drop-precedence

Syntax

remark drop-precedence *drop-precedence-value*

undo remark drop-precedence

View

Traffic behavior view

Default Level

2: System Level

Parameters

drop-precedence-value: Drop precedence to be set for packets, in the range 0 to 2.

Description

Use the **remark drop-precedence** command to configure the action of setting drop precedence for a traffic behavior.

Use the **undo remark drop-precedence** command to remove the action of setting drop precedence.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples

Configure the action to set drop precedence to 2 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark drop-precedence 2
```

remark dscp

Syntax

remark dscp *dscp-value*

undo remark dscp

View

Traffic behavior view

Default Level

2: System Level

Parameters

dscp-value: DSCP precedence to be set for packets, in the range of 0 to 63. This argument can also be the keywords listed in Table 1-4.

Table 1-4 DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
default	000000	0
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
ef	101110	46

Description

Use the **remark dscp** command to configure the action of setting DSCP precedence for a traffic behavior.

Use the **undo remark dscp** command to remove the action of setting DSCP precedence.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples

Configure the action to set DSCP precedence to 6 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dscp 6
```

remark ip-precedence

Syntax

remark ip-precedence *ip-precedence-value*

undo remark ip-precedence

View

Traffic behavior view

Default Level

2: System Level

Parameters

ip-precedence-value: IP precedence to be set for packets, in the range of 0 to 7.

Description

Use the **remark ip-precedence** command to configure the action of setting IP precedence for a traffic behavior.

Use the **undo remark ip-precedence** command to remove the action of setting IP precedence.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples

Configure the action to set IP precedence to 6 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark ip-precedence 6
```

remark local-precedence

Syntax

remark local-precedence *local-precedence*

undo remark local-precedence

View

Traffic behavior view

Default Level

2: System Level

Parameters

local-precedence: Local precedence to be set for packets, in the range of 0 to 7.

Description

Use the **remark local-precedence** command to configure the action of setting local precedence for a traffic behavior.

Use the **undo remark local-precedence** command to remove the action of remarking local precedence.

Note that, when the **remark dot1p** command is used together with the **remark local-precedence** command, the 802.1p precedence to be set for packets must be the same as the local precedence to be set for packets. Otherwise, the corresponding policy cannot be applied successfully.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples

Configure the action to set local precedence to 2 for a traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark local-precedence 2
```

traffic behavior

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

View

System view

Default Level

2: System Level

Parameters

behavior-name: Name of the traffic behavior to be created, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a traffic behavior name.

Description

Use the **traffic behavior** command to create a traffic behavior. This command also leads you to traffic behavior view.

Use the **undo traffic classifier** command to remove a traffic behavior.

Related commands: **qos policy**, **qos apply policy**, **classifier behavior**.

Examples

Define a traffic behavior named behavior1.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1]
```

QoS Policy Configuration Commands

classifier behavior

Syntax

classifier *classifier-name* **behavior** *behavior-name*

undo classifier *classifier-name*

View

Policy view

Default Level

2: System Level

Parameters

classifier-name: Name of an existing class, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a class name.

behavior–name: Name of an existing traffic behavior, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a behavior name.

Description

Use the **classifier behavior** command to associate a traffic behavior with a class.

Use the **undo classifier** command to remove a class from a policy.

Note that each class can be associated with only one traffic behavior.

Related commands: **qos policy**.

Examples

Associate the behavior named *test* with the class named *database* in the policy *user1*.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test
```

display qos policy

Syntax

display qos policy user-defined [*policy-name* [**classifier** *classifier-name*]]

View

Any view

Default Level

1: Monitor level

Parameters

policy-name: Policy name, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a policy name. If no policy is specified, the configuration of all user defined policies is displayed.

classifier-name: Name of a class in the policy, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a class name. If no class is specified, all the classes in the policy are specified.

Description

Use the **display qos policy** command to display the configuration of a user-defined policy, including the configuration of the classes and the associated traffic behaviors in the policy.

Examples

Display the configuration of all the user specified policies.

```
<Sysname> display qos policy user-defined

  User Defined QoS Policy Information:

  Policy: test
   Classifier: test
     Behavior: test
      Accounting Enable
      Committed Access Rate:
        CIR 64 (kbps), CBS 4000 (byte), EBS 4000 (byte), PIR 640 (kbps)
        Green Action: pass
        Red Action: discard
        Yellow Action: pass
```

Table 1-5 display qos policy command output description

Field	Description
Policy	Policy name
Classifier	Class name and the corresponding configuration information
Behavior	Traffic behavior name and the corresponding configuration information

display qos policy global

Syntax

display qos policy global [**slot** *slot-number*] [**inbound**]

View

Any view

Default Level

1: Monitor level

Parameters

inbound: Displays the QoS policy applied globally in the inbound direction of all ports.

slot *slot-number*: Displays the global QoS policy configuration of the specified device in the IRF. If the *slot-number* argument is not specified, the global QoS policy configuration of all devices in the IRF is displayed. If no IRF is formed, the global QoS policy configuration of the current device is displayed. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF.

Description

Use the **display qos policy global** command to display information about a global QoS policy.

Examples

Display information about the global QoS policy in the inbound direction.

```
<Sysname> display qos policy global inbound

  Direction: Inbound

  Policy: abc_policy
   Classifier: abc
     Operator: AND
     Rule(s) : If-match dscp cs1
     Behavior: abc
      Committed Access Rate:
        CIR 640 (kbps), CBS 4000 (byte), EBS 4000 (byte)
        Green Action: pass
        Red Action: discard
        Yellow Action: pass
        Green : 0(Packets)
```

Table 1-6 display qos policy global command output description

Field	Description
Direction	Direction in which the policy is applied globally
Policy	Policy name
Classifier	Class name **Failed** indicates that the policy is not successfully applied
Operator	Logical relationship between match criteria
Rule(s)	Match criteria
Behavior	Name and the corresponding configuration information of a behavior
Committed Access Rate	Rate limiting information
CIR	Committed information rate in kbps
CBS	Committed burst size in bytes, that is, the depth of the token bucket for holding burst traffic
EBS	Excess burst size in bytes, that is, the traffic exceeding CBS when two token buckets are used

Field	Description
Green Action	Action to conduct for green packets
Red Action	Action to conduct for red packets
Yellow Action	Action to conduct for yellow packets
Green	Traffic statistics on green packets

display qos policy interface

Syntax

display qos policy interface [*interface-type interface-number*] [**inbound**]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type: Port type.

interface-number: Port number.

inbound: Specifies the inbound direction.

Description

Use the **display qos policy interface** command to display the configuration and statistics information about the policy applied on a port.

If no interface is provided, the configuration and statistics information about the policies applied on all the ports is displayed.

Examples

Display the configuration and statistics information about the policy applied to port GigabitEthernet 1/0/1.

```
<Sysname> display qos policy interface GigabitEthernet 1/0/1

  Interface: GigabitEthernet1/0/1

  Direction: Inbound

  Policy: abc_policy
   Classifier: abc
     Operator: AND
     Rule(s) : If-match dscp cs1
     Behavior: abc
      Committed Access Rate:
        CIR 64 (kbps), CBS 4000 (byte), EBS 4000 (byte)
```

```
Green Action: pass
Red Action: discard
Yellow Action: pass
Green : 0(Packets)
```

Table 1-7 display qos policy interface command output description

Field	Description
Interface	Port name, comprising of port type and port number
Direction	Direction of the port where the policy is applied
Policy	Name and configuration information of the policy
Classifier	Name and configuration information of the class **Failed** indicates that the policy is not successfully applied
Operator	Logical relationship among the classification rules in a class
Rule(s)	Classification rules in the class
Behavior	Name and configuration information of the behavior

display qos vlan-policy

Syntax

display qos vlan-policy { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-number*] [**inbound**]

View

Any view

Default Level

1: Monitor level

Parameters

name *policy-name*: Specifies to display the information about the VLAN policy with the specified name, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a VLAN policy name.

vlan *vlan-id*: Specifies to display the information about the VLAN policy applied to the specified VLAN. If no VLAN ID is specified, the VLAN policy information of all VLANs is displayed.

slot-number: Specifies to display VLAN QoS policy information about the specified device in the IRF. If the *slot-number* argument is not specified, the VLAN QoS policy information of all devices in the IRF is displayed. If no IRF is formed, the VLAN QoS policy information of the current device is displayed. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF.

Description

Use the **display qos vlan-policy** command to display the information about VLAN QoS policies.

Examples

Display the information about the VLAN QoS policy **test**.

```
<Sysname> display qos vlan-policy name test
```

```
Policy test
  Vlan 300: inbound
```

Table 1-8 display qos vlan-policy command output description

Field	Description
Policy	Name of the VLAN policy
Vlan 300	ID of the VLAN where the VLAN policy is applied
inbound	VLAN policy is applied in the inbound direction of the VLAN.

Display the information about the VLAN policy applied to VLAN 300.

```
<Sysname> display qos vlan-policy vlan 300

  Vlan 300

  Direction: Inbound

  Policy: test
   Classifier: test
     Operator: AND
     Rule(s) : If-match customer-vlan-id 3
     Behavior: test
      Accounting Enable:
        0 (Packets)
      Committed Access Rate:
        CIR 6400 (kbps), CBS 4000 (byte), EBS 4000 (byte)
        Green Action: pass
        Red Action: discard
        Yellow Action: pass
        Green : 0(Packets)
```

Table 1-9 display qos vlan-policy command output description

Field	Description
Vlan 300	ID of the VLAN where the VLAN policy is applied
Inbound	VLAN policy is applied in the inbound direction of the VLAN.
Classifier	Name of the class in the policy and its configuration
Operator	Logical relationship between classification rules
Rule(s)	Classification rules
Behavior	Name of the behavior in the policy and its configuration
Accounting	Traffic accounting action
Committed Access Rate	Rate limiting information
CIR	Committed information rate in kbps
CBS	Committed burst size in bytes, that is, the depth of the token bucket for holding burst traffic

Field	Description
EBS	Excess burst size in bytes, namely, the traffic exceeding CBS when two token buckets are used
Green Action	Action to conduct for green packets
Red Action	Action to conduct for red packets
Yellow Action	Action to conduct for yellow packets
Green	Traffic statistics about green packets

qos apply policy

Syntax

qos apply policy *policy-name* **inbound**

undo qos apply policy inbound

View

Ethernet interface view, port group view

Default Level

2: System Level

Parameters

inbound: Specifies the inbound direction.

policy-name: Specifies a QoS policy name, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a QoS policy name.

Description

Use the **qos apply policy** command to apply a QoS policy on a port or a port group.

Use the **undo qos apply policy** command to remove the policy applied on a port or a port group.

Examples

Apply the policy named test in the inbound direction of GigabitEthernet1/0/1 port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos apply policy test inbound
```

qos apply policy global

Syntax

qos apply policy *policy-name* **global inbound**

undo qos apply policy global inbound

View

System view

Default Level

2: System Level

Parameters

policy-name: Policy name, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a QoS policy name.

inbound: Applies the QoS policy to the incoming packets on all ports.

Description

Use the **qos apply policy global** command to apply a QoS policy globally. A QoS policy applied globally takes effect on all inbound traffic depending on the direction in which the policy is applied.

Use the **undo qos apply policy global** command to cancel the global application of the QoS policy.

Examples

Apply the QoS policy **user1** in the inbound direction globally.

```
<Sysname> system-view
[Sysname] qos apply policy user1 global inbound
```

qos policy

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

View

System view

Default Level

2: System Level

Parameters

policy-name: Name of the policy to be created, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a policy name.

Description

Use the **qos policy** command to create a policy. This command also leads you to policy view.

Use the **undo qos policy** command to remove a policy.

To remove a policy that is currently applied on a port, you need to disable it on the port first.

Related commands: **classifier behavior**, **qos apply policy**.

Examples

Create a policy named user1.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1]
```

qos vlan-policy

Syntax

qos vlan-policy *policy-name* **vlan** *vlan-id-list* **inbound**

undo qos vlan-policy vlan *vlan-id-list* **inbound**

View

System view

Default Level

2: System Level

Parameters

policy-name: Policy name, a case-sensitive string of 1 to 31 characters. No spaces are allowed in a policy name.

vlan-id-list: List of VLAN IDs, presented in the form of *vlan-id* **to** *vlan-id* or discontinuous VLAN IDs. Up to eight VLAN IDs can be specified at a time.

inbound: Specifies to apply the VLAN policy in the inbound direction of the VLAN.

Description

Use the **qos vlan-policy** command to apply the VLAN policy to the specific VLAN(s).

Use the **undo qos vlan-policy** command to remove the VLAN policy from the specific VLAN(s).

 **Note**

Do not apply policies to a VLAN and the ports in the VLAN at the same time.

Examples

Apply the VLAN policy named test in the inbound direction of VLAN 200, VLAN 300, VLAN 400, VLAN 500, VLAN 600, VLAN 700, VLAN 800, and VLAN 900.

```
<Sysname> system-view
[Sysname] qos vlan-policy test vlan 200 300 400 500 600 700 800 900 inbound
```

reset qos policy global

Syntax

reset qos policy global [**inbound**]

View

User view

Default Level

1: Monitor level

Parameters

inbound: Specifies the inbound direction.

Description

Use the **reset qos vlan-policy** command to clear the statistics of a global QoS policy. If no direction is specified, all global QoS policy statistics are cleared.

Examples

Clear the statistics of the global QoS policy in the inbound direction.

```
<Sysname> reset qos policy global inbound
```

reset qos vlan-policy

Syntax

reset qos vlan-policy [**vlan** *vlan-id*] [**inbound**]

View

User view

Default Level

1: Monitor level

Parameters

vlan-id: VLAN ID, in the range 1 to 4,094.

inbound: Clears the QoS policy statistics in the inbound direction of the specified VLAN.

Description

Use the **reset qos vlan-policy** command to clear the statistics information about VLAN QoS policies.

If no VLAN ID is specified, QoS policy statistics of all VLANs are cleared.

Examples

Clear the statistics information about the QoS policy applied to VLAN 2.

```
<Sysname> reset qos vlan-policy vlan 2
```

2 Priority Mapping Configuration Commands

Priority Mapping Table Configuration Commands

display qos map-table

Syntax

display qos map-table [**dot1p-dp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp**]

View

Any view

Default Level

1: Monitor level

Parameters

dot1p-lp: Specifies the 802.1p precedence-to-local precedence mapping table.

dot1p-dp: Specifies the 802.1p precedence-to-drop precedence mapping table.

dscp-dp: Specifies the DSCP-to-drop precedence mapping table.

dscp-dot1p: Specifies the DSCP-to-802.1p precedence mapping table.

dscp-dscp: Specifies the DSCP-to-DSCP mapping table.

Description

Use the **display qos map-table** command to display the configuration of a priority mapping table.

If the type of the priority mapping table is not specified, the configuration of all the priority mapping tables is displayed.

Related commands: **qos map-table**.

Examples

Display the configuration of the 802.1p precedence-to-drop precedence mapping table.

```
<Sysname> display qos map-table dot1p-dp
MAP-TABLE NAME: dot1p-dp   TYPE: pre-define
IMPORT  :  EXPORT
  0    :    2
  1    :    2
  2    :    2
  3    :    1
  4    :    1
  5    :    1
  6    :    0
  7    :    0
```

Table 2-1 display qos map-table command output description

Field	Description
MAP-TABLE NAME	Name of the mapping table
TYPE	Type of the mapping table
IMPORT	Input entries of the mapping table
EXPORT	Output entries of the mapping table

qos map-table

Syntax

qos map-table { **dot1p-dp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** }

View

System view

Default Level

2: System Level

Parameters

dot1p-lp: Specifies the 802.1p precedence-to-local precedence mapping table.

dot1p-dp: Specifies the 802.1p precedence-to-drop precedence mapping table.

dscp-dp: Specifies the DSCP-to-drop precedence mapping table.

dscp-dot1p: Specifies the DSCP-to-802.1p precedence mapping table.

dscp-dscp: Specifies the DSCP-to-DSCP mapping table.

Description

Use the **qos map-table** command to enter specific priority mapping table view.

Related commands: **display qos map-table**.

Examples

Enter 802.1p precedence-to-drop precedence mapping table view.

```
<Sysname> system-view
[Sysname] qos map-table dot1p-dp
[Sysname-maptbl-dot1p-dp]
```

import

Syntax

import *import-value-list* **export** *export-value*

undo import { *import-value-list* | **all** }

View

Priority mapping table view

Default Level

2: System Level

Parameters

import-value-list: List of input parameters, in the range of 0 to 7.

export-value: Output parameter in the mapping table, in the range of 0 to 2.

all: Removes all the parameters in the priority mapping table.

Description

Use the **import** command to configure entries for a priority mapping table, that is, to define one or more mapping rules.

Use the **undo import** command to restore specific entries of a priority mapping table to the default.

Note that, you cannot configure to map any DSCP value to drop precedence 1.

Related commands: **display qos map-table**.

Examples

Configure the 802.1p precedence-to-drop precedence mapping table to map 802.1p precedence 4 and 5 to drop precedence 1.

```
<Sysname> system-view
[Sysname] qos map-table dot1p-dp
[Sysname-maptbl-dot1p-dp] import 4 5 export 1
```

Port Priority Configuration Commands

qos priority

Syntax

qos priority *priority-value*

undo qos priority

View

Ethernet interface view, port group view

Default Level

2: System Level

Parameters

priority-value: Port priority to be configured. This argument is in the range 0 to 7.

Description

Use the **qos priority** command to set the port priority for a port.

Use the **undo qos priority** command to restore the default port priority.

By default, the port priority is 0.

Note that, if a port receives packets without an 802.1q tag, the switch takes the priority of the receiving port as the 802.1p precedence of the packets and then searches the **dot1p-dp/lp** mapping table for the local/drop precedence for the packets according to the priority of the receiving port.

Examples

Set the port priority of GigabitEthernet1/0/1 port to 2.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos priority 2
```

Port Priority Trust Mode Configuration Commands

display qos trust interface

Syntax

display qos trust interface [*interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type: Port type.

interface-number: Port number.

Description

Use the **display qos trust interface** command to display the port priority trust mode of a port.

If no port is specified, this command displays the port priority trust modes of all the ports.

Examples

Display the port priority trust mode of GigabitEthernet1/0/1 port.

```
<Sysname> display qos trust interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
Port priority information
Port priority :0
Port priority trust type : dscp
```

Table 2-2 display qos trust interface command output description

Field	Description
Interface	Port name, comprising of port type and port number
Port priority	Port priority

Field	Description
Port priority trust type	Port priority trust mode • dscp indicates that the DSCP precedence of the received packets is trusted • dot1p indicates that the 802.1p precedence of the received packets is trusted • untrust indicates that the port priority is trusted

qos trust

Syntax

qos trust { **dot1p** | **dscp** }

undo qos trust

View

Ethernet interface view, port group view

Default Level

2: System Level

Parameters

dscp: Specifies to trust DSCP precedence carried in the packet and adopt this priority for priority mapping.

dot1p: Specifies to trust 802.1p precedence carried in the packet and adopt this priority for priority mapping.

Description

Use the **qos trust** command to configure the port priority trust mode.

Use the **undo qos trust** command to restore the default port priority trust mode.

By default, the port priority is trusted.

Examples

Specify to trust the DSCP precedence carried in packets on GigabitEthernet1/0/1 port.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos trust dscp
```

3 Traffic Shaping and Line Rate Configuration Commands

Traffic Shaping Configuration Commands

display qos gts interface

Syntax

display qos gts interface [*interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type: Port type.

interface-number: Port number.

Description

Use the **display qos gts interface** command to display traffic shaping configuration information.

If no port is specified, traffic shaping configuration information of all ports is displayed.

Examples

Display traffic shaping configuration information of all ports.

```
<Sysname> display qos gts interface
Interface: GigabitEthernet1/0/1
Rule(s): If-match queue 2
 CIR 640 (kbps), CBS 40960 (byte)
```

Table 3-1 display qos gts command output description

Field	Description
Interface	Port name identified by port type and port number
Rule(s)	Match criteria. “If-match queue 2” indicates that traffic shaping is performed for traffic in queue 2.
CIR	Committed information rate (CIR) in kbps
CBS	Committed burst size (CBS) in bytes

qos gts

Syntax

qos gts queue *queue-number* **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos gts queue *queue-number*

View

Ethernet interface view, port group view

Default Level

2: System level

Parameters

queue *queue-number*: Specifies a queue by its number, which ranges from 0 to 7.

cir *committed-information-rate*: Specifies the committed information rate (CIR) in kbps, which must be a multiple of 64, and CIR ranges from 64 to 16777216.

cbs *committed-burst-size*: Specifies the CBS (in bytes), which ranges from 4096 to 16777216 and must be a multiple of 4096.

If the **cbs** keyword is not specified, the default CBS is 62.5 ms × *committed-information-rate* and must be a multiple of 4096. If 62.5 ms × *committed-information-rate* is not a multiple of 4096, the default CBS is the multiple of 4096 that is bigger than and nearest to 62.5 ms × *committed-information-rate*. The maximum CBS is 16777216. For example, if the CIR is 640 kbps, then 62.5 ms × CIR is 62.5 ms × 640 = 40000. As 40000 is not a multiple of 4096, 40960, which is the multiple of 4096 that is bigger than and nearest to 40000, is taken as the default CBS.

Description

Use the **qos gts** command to configure traffic shaping.

Use the **undo qos gts** command to remove the traffic shaping configuration.

In Ethernet interface view, the configuration takes effect on the current port. In port group view, the configuration takes effect on all ports in the port group.

Examples

Configure traffic shaping on GigabitEthernet 1/0/1 to limit the outgoing traffic rate of queue 2 to 640 kbps.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos gts queue 2 cir 640
```

Line Rate Configuration Commands

display qos lr interface

Syntax

display qos lr interface [*interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type: Port type.

interface-number: Port number.

Description

Use the **display qos lr interface** command to display the line rate configuration information of the specified port or all ports if no port is specified.

Examples

Display the line rate configuration and statistics information of all the interfaces.

```
<Sysname> display qos lr interface
Interface: GigabitEthernet1/0/1
Direction: Inbound
 CIR 6400 (kbps),  CBS 400000 (byte)
```

Table 3-2 display qos lr command output description

Field	Description
Interface	Port name, composed of port type and port number
Direction	Specify the direction of limited rate as inbound
CIR	Committed information rate, in kbps
CBS	Committed burst size, in byte

qos lr outbound

Syntax

qos lr outbound cir *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos lr outbound

View

Ethernet interface view, port group view

Default Level

2: System Level

Parameters

outbound: Limits the rate of the outbound traffic.

cir *committed-information-rate*: Specifies the committed information rate (CIR) in kbps. The range of CIR varies with port types as follows:

- GigabitEthernet port: 64 to 1000000
- Ten-GigabitEthernet port: 64 to 10000000

Note that the *committed-information-rate* argument must be a multiple of 64.

cbs *committed-burst-size*: Specifies the committed burst size in bytes.

- The *committed-burst-size* argument ranges from 4000 to 16000000.
- If the **cbs** keyword is not used, the system uses the default committed burst size, that is, 62.5 ms x *committed-information-rate,* or 16000000 if the multiplication is more than 16000000.

Description

Use the **qos lr outbound** command to limit the rate of outbound traffic via physical interfaces.

Use the **undo qos lr outbound** command to cancel the limit.

Examples

Limit the outbound traffic rate on GigabitEthernet 1/0/1 within 640 kbps.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos lr outbound cir 640
```

4 Congestion Management Configuration Commands

Congestion Management Configuration Commands

display qos sp interface

Syntax

display qos sp interface [*interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type: Port type.

interface-number: Port number.

Description

Use the **display qos sp interface** command to display the strict priority (SP) queuing configuration on a specified port.

If no port is specified, this command displays the SP queuing configuration on all ports.

Related commands: **qos sp**.

Examples

Display the SP queuing configuration on GigabitEthernet 1/0/1.

```
<Sysname> display qos sp interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
Output queue: Strict-priority queue
```

display qos wfq interface

Syntax

display qos wfq interface [*interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type: Port type.

interface-number: Port number.

Description

Use the **display qos wfq interface** command to display the configuration of Weighted Fair Queuing (WFQ) queues of a port.

If no port number is specified, the command displays the configurations of WFQ queues of all ports.

Related commands: **qos wfq**.

Examples

Display the configuration of the WFQ queues on port GigabitEthernet 1/0/1.

```
<Sysname> display qos wfq interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
Output queue: Hardware weighted fair queue
Queue ID        Weight         Min-Bandwidth
-----------------------------------------------
0               1              64
1               2              64
2               4              64
3               6              64
4               8              64
5              10              64
6              12              64
7              14              64
```

Table 4-1 display qos wfq interface command output description

Field	Description
Interface	Port name, composed of port type and port number
Output queue	The type of the current output queue
Queue ID	ID of the queue
Weight	The weight of each queue during scheduling.
Min-Bandwidth	Minimum guaranteed bandwidth of the queue

display qos wrr interface

Syntax

display qos wrr interface [*interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type: Port type.

interface-number: Port number.

Description

Use the **display qos wrr interface** command to display the configuration of weighted round robin (WRR) queues of a port.

If no port number is specified, the command displays the configurations of WRR queues of all ports.

Related commands: **qos wrr**.

Examples

Display the configuration of WRR queues of GigabitEthernet 1/0/1.

```
<Sysname> display qos wrr interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
Output queue:   Weighted round robin queue
Queue ID    Group    Weight
-------------------------------------
  0         sp       N/A
  1         sp       N/A
  2         1        3
  3         1        4
  4         1        5
  5         1        6
  6         1        7
  7         1        8
```

Table 4-2 display qos wrr interface command output description

Field	Description
Interface	Port name, composed of port type and port number
Output queue	The type of the current output queue
Queue ID	ID of the queue
Group	Group ID, indicating which group a queue belongs to.
Weight	The weight of each queue during scheduling. N/A indicates that SP queue scheduling algorithm is adopted.

qos bandwidth queue

Syntax

qos bandwidth queue *queue-id* **min** *bandwidth-value*

undo qos bandwidth queue *queue-id* [**min** *bandwidth-value*]

View

Ethernet interface view, port group view

Default Level

2: System level

Parameters

queue-id: Queue ID, in the range of 0 to 7.

bandwidth-value: Minimum guaranteed bandwidth (in kbps), that is, the minimum bandwidth guaranteed for a queue when the port is congested. The range for the *bandwidth-value* argument is 64 to 1048576.

Description

Use the **qos bandwidth queue** command to set the minimum guaranteed bandwidth for a specified queue on the port or ports in the port group.

Use the **undo qos bandwidth queue** command to remove the configuration.

By default, the minimum guaranteed bandwidth of a queue is 64 kbps.

Note that:

- In Ethernet interface view, the configuration takes effect only on the current port; in port group view, the configuration takes effect on all ports in the port group.
- To configure minimum guaranteed bandwidth for queues on a port/port group, enable WFQ on the port/port group first.

Examples

Set the minimum guaranteed bandwidth to 100 kbps for queue 0 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet 1/0/1] qos wfq
[Sysname-GigabitEthernet 1/0/1] qos bandwidth queue 0 min 100
```

qos sp

Syntax

qos sp

undo qos sp

View

Ethernet interface view, port group view

Default Level

2: System Level

Parameters

None

Description

Use the **qos sp** command to configure SP queuing on the current port.

Use the **undo qos sp** command to restore the default queuing algorithm on the port.

By default, all the ports adopt the WRR queue scheduling algorithm, with the weight values assigned to queue 0 through queue 7 being 1, 2, 3, 4, 5, 9, 13, and 15.

Related commands: **display qos sp interface**.

Examples

Configure SP queuing on GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos sp
```

qos wfq

Syntax

qos wfq

undo qos wfq

View

Ethernet interface view, port group view

Default Level

2: System Level

Parameters

None

Description

Use the **qos wfq** command to enable weighted fair queuing (WFQ) on a port or port group.

Use the **undo qos wfq** command to restore the default.

By default, all the ports adopt the WRR queue scheduling algorithm, with the weight values assigned to queue 0 through queue 7 being 1, 2, 3, 4, 5, 9, 13, and 15.

Related commands: **display qos wrr interface**.

Examples

Enable WFQ on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] qos wfq
```

qos wfq weight

Syntax

qos wfq *queue-id* **weight** *schedule-value*

undo qos wfq *queue-id* **weight**

View

Ethernet interface view, port group view

Default Level

2: System Level

Parameters

queue-id: ID of the queue, in the range of 0 to 7.

weight *schedule-value*: Specifies the scheduling weight of a queue, ranges from 0 to 15, and each queue is allocated with part of the allocable bandwidth based on its scheduling weight.

Description

Use the **qos wfq** command to enable weighted fair queuing (WFQ) on a port or port group and configure a scheduling weight for the specified queue.

Use the **undo qos wfq** command to restore the default.

On a WFQ-enable port/port group, the scheduling weight of a queue is 1 by default.

Related commands: **display qos wfq interface**, **qos bandwidth queue**.

Examples

Enable WFQ on GigabitEthernet 1/0/1 and assign weight values 1, 2, 4, 6, 8, 10, 12, and 14 to queues 0 through 7.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq
[Sysname-GigabitEthernet1/0/1] qos wfq 0 weight 1
[Sysname-GigabitEthernet1/0/1] qos wfq 1 weight 2
[Sysname-GigabitEthernet1/0/1] qos wfq 2 weight 4
[Sysname-GigabitEthernet1/0/1] qos wfq 3 weight 6
[Sysname-GigabitEthernet1/0/1] qos wfq 4 weight 8
[Sysname-GigabitEthernet1/0/1] qos wfq 5 weight 10
[Sysname-GigabitEthernet1/0/1] qos wfq 6 weight 12
[Sysname-GigabitEthernet1/0/1] qos wfq 7 weight 14
```

qos wrr

Syntax

qos wrr

undo qos wrr

View

Ethernet interface view, port group view

Default Level

2: System Level

Parameters

None

Description

Use the **qos wrr** command to enable weighted round robin (WRR) on a port or port group.

Use the **undo qos wrr** command to restore the default.

By default, all the ports adopt the WRR queue scheduling algorithm, with the weight values assigned to queue 0 through queue 7 being 1, 2, 3, 4, 5, 9, 13, and 15.

Related commands: **display qos wrr interface**.

Examples

Enable WRR on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
```

qos wrr group

Syntax

qos wrr *queue-id* **group** { **sp** | *group-id* **weight** *schedule-value* }

undo qos wrr

View

Ethernet interface view, port group view

Default Level

2: System Level

Parameters

queue-id: ID of the queue, in the range of 0 to 7.

group-id: It can only be 1.

weight *schedule-value*: Specifies the scheduling weight of a queue, rang from 1 to 15.

sp: Configures SP queuing.

Description

Use the **qos wrr** command to configure Weighted Round Robin (WRR) queue scheduling algorithm or the SP + WRR queue scheduling algorithm on a port or port group.

Use the **undo qos wrr** command to restore the default queue-scheduling algorithm on the port.

By default, all the ports adopt the WRR queue scheduling algorithm, with the weight values assigned to queue 0 through queue 7 being 1, 2, 3, 4, 5, 9, 13, and 15.

As required, you can configure part of the queues on the port to adopt the SP queue-scheduling algorithm and parts of queues to adopt the WRR queue-scheduling algorithm. Through adding the queues on a port to the SP scheduling group and WRR scheduling group (namely, group 1), the SP + WRR queue scheduling is implemented. During the queue scheduling process, the queues in the SP scheduling group is scheduled preferentially. When no packet is to be sent in the queues in the SP scheduling group, the queues in the WRR scheduling group are scheduled. The queues in the SP scheduling group are scheduled according to the strict priority of each queue, while the queues in the WRR queue scheduling group are scheduled according the weight value of each queue.

Related commands: **display qos wrr interface**.

Examples

Configure SP+WRR queue scheduling algorithm on GigabitEthernet 1/0/1 as follows: assign queue 0, queue 1, queue 2, and queue 3 to the SP scheduling group; and assign queue 4, queue 5, queue 5, and queue 7 to WRR scheduling group, with the weight 2, 4, 6, and 8.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 1 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 2 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 3 group sp
[Sysname-GigabitEthernet1/0/1] qos wrr 4 group 1 weight 2
[Sysname-GigabitEthernet1/0/1] qos wrr 5 group 1 weight 4
[Sysname-GigabitEthernet1/0/1] qos wrr 6 group 1 weight 6
[Sysname-GigabitEthernet1/0/1] qos wrr 7 group 1 weight 8
```

5 Traffic Mirroring Configuration Commands

Traffic Mirroring Configuration Commands

mirror-to

Syntax

mirror-to { **cpu | interface** *interface-type interface-number* }

undo mirror-to { **cpu | interface** *interface-type interface-number* }

View

Traffic behavior view

Default Level

2: System Level

Parameters

cpu: Redirects packets to the CPU.

interface *interface-type interface-number*: Port type and port number of the destination port for the traffic mirroring action.

Description

Use the **mirror-to** command to configure traffic mirroring action for a traffic behavior.

Use the **undo mirror-to** command to remove the traffic mirroring action.

Examples

Configure traffic behavior 1 and define the action of mirroring traffic to GigabitEthernet1/0/2 in the traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior 1
[Sysname-behavior-1] mirror-to interface GigabitEthernet 1/0/2
```

6 User Profile Configuration Commands

User Profile Configuration Commands

display user-profile

Syntax

display user-profile

View

Any view

Default Level

2: System level

Parameters

None

Description

Use the **display user-profile** command to display information of all the user profiles that have been created.

Examples

Display information of all the user profiles that have been created.

```
<Sysname> display user-profile
Status     User profile                    AuthType
enabled    b123                            DOT1X
       ----Total user profiles:       1-------
       ----Enabled user profiles:     1-------
```

Table 6-1 display user-profile command output description

Field	Description
Status	Status of the current user profile: • enabled • disabled
User profile	User profile name
AuthType	Authentication type of the current user profile
Total user profiles	Total number of user profiles that have been created
Enabled user profiles	Total number of user profiles that have been enabled

user-profile enable

Syntax

user-profile *profile-name* **enable**

undo user-profile *profile-name* **enable**

View

System view

Default Level

2: System level

Parameters

profile-name: Use profile name, a string of 1 to 31 characters, case sensitive. It can only contain English letters, numbers, underlines, and must start with an English letter.

Description

Use the **user-profile enable** command to enable a user profile.

Use the **undo user-profile enable** command to disable the specified user profile.

By default, a created user profile is disabled.

Note that:

- When you execute the command, the specified user profile must be created; otherwise, the command fails.
- Only an enabled user profile can be used by users. You cannot modify or remove the configuration items in a user profile until the user profile is disabled.
- Disabling a user profile logs out the users using the user profile.

Examples

Enable user profile **a123**.

```
<Sysname> system-view
[Sysname] user-profile a123 enable
```

user-profile

Syntax

user-profile *profile-name* [**dot1x**]

undo user-profile *profile-name* [**dot1x**]

View

System view

Default Level

2: System level

Parameters

profile-name: Use profile name, a string of 1 to 31 characters, case sensitive. It can only contain English letters, numbers, underlines, and must start with an English letter. A user profile name must be globally unique.

dot1x: Uses 802.1X authentication when users access the device. Refer to *802.1X Configuration* in the *Security Volume* for the detailed information about 802.1X.

Description

Use the **user-profile** command to create a user profile and enter the corresponding user profile view. If the specified user profile already exists, you will directly enter the corresponding user profile view, without the need to create a user profile. Use the **undo user-profile** command to remove an existing, disabled user profile.

By default, no user profiles exist on the device.

Note that:

- The **dot1x** keyword is required when you creating a user profile, and it's optional when you entering the user profile view or deleting an existing user profile.
- An enabled user profile cannot be removed.

Related commands: **user-profile enable**.

Examples

Create a user profile **a123**, using 802.1X authentication.

```
<Sysname> system-view
[Sysname] user-profile a123 DOT1X
[Sysname-user-profile-DOT1X-a123]
```

Enter the corresponding user profile view of **a123**.

```
<Sysname> system-view
[Sysname] user-profile a123
[Sysname-user-profile-DOT1X-a123]
```

Table of Contents

1 AAA Configuration Commands

AAA Configuration Commands

access-limit enable

Syntax

access-limit enable *max-user-number*

undo access-limit enable

View

ISP domain view

Default Level

2: System level

Parameters

max-user-number: Maximum number of user connections for the current ISP domain. The valid range from 1 to 2147483646.

Description

Use the **access-limit enable** command to enable the limit on the number of user connections in an ISP domain and set the allowed maximum number. After the number of user connections reaches the maximum number allowed, no more users will be accepted.

Use the **undo access-limit enable** command to restore the default.

By default, there is no limit to the number of user connections in an ISP domain.

As user connections may compete for network resources, setting a proper limit to the number of user connections helps provide a reliable system performance.

Examples

Set a limit of 500 user connections for ISP domain **aabbcc.net**.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] access-limit enable 500
```

access-limit

Syntax

access-limit *max-user-number*

undo access-limit

View

Local user view

Default Level

3: Manage level

Parameters

max-user-number: Maximum number of user connections using the current username, in the range 1 to 1024.

Description

Use the **access-limit** command to enable the limit on the number of user connections using the current username and set the allowed maximum number.

Use the **undo access-limit** command to remove the limitation.

By default, there is no limit to the number of user connections using the same username.

Note that the **access-limit** command takes effect only when local accounting is configured.

Related commands: **display local-user**.

Examples

Enable the limit on the number of user connections using the username **abc** and set the allowed maximum number to 5.

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] access-limit 5
```

accounting command

Syntax

accounting command hwtacacs-scheme *hwtacacs-scheme-name*

undo accounting command

View

ISP domain view

Default Level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

Description

Use the **accounting command** command to specify the HWTACACS scheme for command line users.

Use the **undo accounting command** command to restore the default.

By default, the default accounting method that the **accounting default** command prescribes is used for command line users.

Note that:

- The HWTACACS scheme specified for the current ISP domain must have been configured.
- Currently, only HWTACACS schemes support command line accounting.

Related commands: **accounting default**, **hwtacacs scheme**.

Examples

Configure the ISP domain **test** to use HWTACACS scheme **hw** for accounting of command line users.

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting command hwtacacs-scheme hw
```

accounting default

Syntax

accounting default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting default

View

ISP domain view

Default Level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description

Use the **accounting default** command to configure the default accounting method for all types of users.

Use the **undo accounting default** command to restore the default.

By default, the accounting method is **local**.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- The accounting method configured with the **accounting default** command is for all types of users and has a priority lower than that for a specific access mode.

- Local accounting is only for managing the local user connection number; it does not provide the statistics function. The local user connection number management is only for local accounting; it does not affect local authentication and authorization.

Related commands: **authentication default**, **authorization default**, **hwtacacs scheme**, **radius scheme**.

Examples

Configure the default ISP domain **system** to use the local accounting method for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting default local
```

Configure the default ISP domain **system** to use RADIUS accounting scheme **rd** for all types of users and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting default radius-scheme rd local
```

accounting lan-access

Syntax

accounting lan-access { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting lan-access

View

ISP domain view

Default Level

2: System level

Parameters

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description

Use the **accounting lan-access** command to configure the accounting method for LAN access users.

Use the **undo accounting lan-access** command to restore the default.

By default, the default accounting method that the **accounting default** command prescribes is used for LAN access users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related commands: **accounting default**, **radius scheme**.

Examples

Configure the default ISP domain **system** to use the local accounting method for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting lan-access local
```

Configure the default ISP domain **system** to use RADIUS accounting scheme **rd** for LAN access users and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting lan-access radius-scheme rd local
```

accounting login

Syntax

accounting login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting login

View

ISP domain view

Default Level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local accounting. It is not used for charging purposes, but for collecting statistics on and limiting the number of local user connections.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description

Use the **accounting login** command to configure the accounting method for login users.

Use the **undo accounting login** command to restore the default.

By default, the default accounting method is used for login users.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- Accounting is not supported for login users' FTP services.

Related commands: **accounting default**, **hwtacacs scheme**, **radius scheme**.

Examples

Configure the default ISP domain **system** to use the local accounting method for login users.

```
<Sysname> system-view
[Sysname] domain system
```

```
[Sysname-isp-system] accounting login local
```

Configure the default ISP domain **system** to use RADIUS accounting scheme **rd** for login users and use local accounting as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting login radius-scheme rd local
```

accounting optional

Syntax

accounting optional

undo accounting optional

View

ISP domain view

Default Level

2: System level

Parameters

None

Description

Use the **accounting optional** command to enable the accounting optional feature.

Use the **undo accounting optional** command to disable the feature.

By default, the feature is disabled.

Note that with the **accounting optional** command configured for a domain:

- A user that will be disconnected otherwise can use the network resources even when there is no accounting server available or communication with the current accounting server fails. This command applies to scenarios where authentication is required but accounting is not.
- If accounting for a user in the domain fails, the device will not send real-time accounting updates for the user any more.
- The limit on the number of local user connections configured by using the **access-limit** command in local user view is not effective.

Examples

Enable the accounting optional feature for users in domain **aabbcc.net**.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] accounting optional
```

authentication default

Syntax

authentication default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication default

View

ISP domain view

Default Level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description

Use the **authentication default** command to configure the default authentication method for all types of users.

Use the **undo authentication default** command to restore the default.

By default, the authentication method is **local**.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- The authentication method specified with the **authentication default** command is for all types of users and has a priority lower than that for a specific access mode.

Related commands: **authorization default**, **accounting default**, **hwtacacs scheme**, **radius scheme**.

Examples

Configure the default ISP domain **system** to use local authentication for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication default local
```

Configure the default ISP domain **system** to use RADIUS authentication scheme **rd** for all types of users and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication default radius-scheme rd local
```

authentication lan-access

Syntax

authentication lan-access { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication lan-access

View

ISP domain view

Default Level

2: System level

Parameters

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description

Use the **authentication lan-access** command to configure the authentication method for LAN access users.

Use the **undo authentication login** command to restore the default.

By default, the default authentication method is used for LAN access users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related commands: **authentication default**, **radius scheme**.

Examples

Configure the default ISP domain **system** to use local authentication for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication lan-access local
```

Configure the default ISP domain **system** to use RADIUS authentication scheme **rd** for LAN access users and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication lan-access radius-scheme rd local
```

authentication login

Syntax

authentication login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication login

View

ISP domain view

Default Level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description

Use the **authentication login** command to configure the authentication method for login users.

Use the **undo authentication login** command to restore the default.

By default, the default authentication method is used for login users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

Related commands: **authentication default**, **hwtacacs scheme**, **radius scheme**.

Examples

Configure the default ISP domain **system** to use local authentication for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication login local
```

Configure the default ISP domain **system** to use RADIUS authentication scheme **rd** for login users and use local authentication as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication login radius-scheme rd local
```

authorization command

Syntax

authorization command { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local** | **none**] | **local** | **none** }

undo authorization command

View

ISP domain view

Default Level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the corresponding default rights.

Description

Use the **authorization command** command to configure the authorization method for command line users.

Use the **undo authorization command** command to restore the default.

By default, the default authorization method is used for command line users.

Note that:

- The HWTACACS scheme specified for the current ISP domain must have been configured.
- For local authorization, the local users must have been configured for the command line users on the device, and the level of the commands authorized to a local user must be lower than or equal to that of the local user. Otherwise, local authorization will fail.

Related commands: **authorization default**, **hwtacacs scheme**.

Examples

Configure the default ISP domain **system** to use HWTACACS authorization scheme **hw** for command line users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization command hwtacacs-scheme hw
```

Configure the default ISP domain **system** to use HWTACACS authorization scheme **hw** for command line users and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization command hwtacacs-scheme hw local
```

authorization default

Syntax

authorization default { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization default

View

ISP domain view

Default Level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the corresponding default rights.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description

Use the **authorization default** command to configure the authorization method for all types of users.

Use the **undo authorization default** command to restore the default.

By default, the authorization method for all types of users is **local**.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- The authorization method specified with the **authorization default** command is for all types of users and has a priority lower than that for a specific access mode.
- RADIUS authorization is special in that it takes effect only when the RADIUS authorization scheme is the same as the RADIUS authentication scheme. If the RADIUS authorization scheme is different from the RADIUS authentication scheme, RADIUS authorization will fail. In addition, if a RADIUS authorization fails, the error message returned to the NAS says that the server is not responding.

Related commands: **authentication default**, **accounting default**, **hwtacacs scheme**, **radius scheme**.

Examples

Configure the default ISP domain **system** to use local authorization for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization default local
```

Configure the default ISP domain **system** to use RADIUS authorization scheme **rd** for all types of users and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization default radius-scheme rd local
```

authorization lan-access

Syntax

authorization lan-access { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization lan-access

View

ISP domain view

Default Level

2: System level

Parameters

local: Performs local authorization.

none: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default rights.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description

Use the **authorization lan-access** command to configure the authorization method for LAN access users.

Use the **undo authorization lan-access** command to restore the default.

By default, the default authorization method is used for LAN access users.

Note that:

- The RADIUS scheme specified for the current ISP domain must have been configured.
- RADIUS authorization is special in that it takes effect only when the RADIUS authorization scheme is the same as the RADIUS authentication scheme. If the RADIUS authorization scheme is different from the RADIUS authentication scheme, RADIUS authorization will fail.

Related commands: **authorization default**, **radius scheme**.

Examples

Configure the default ISP domain **system** to use local authorization for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system]authorization lan-access local
```

Configure the default ISP domain **system** to use RADIUS authorization scheme **rd** for LAN access users and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization lan-access radius-scheme rd local
```

authorization login

Syntax

authorization login { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization login

View

ISP domain view

Default Level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default rights.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description

Use the **authorization login** command to configure the authorization method for login users.

Use the **undo authorization login** command to restore the default.

By default, the default authorization method is used for login users.

Note that:

- The RADIUS, HWTACACS, or LDAP scheme specified for the current ISP domain must have been configured.
- RADIUS authorization is special in that it takes effect only when the RADIUS authorization scheme is the same as the RADIUS authentication scheme. If the RADIUS authorization scheme is different from the RADIUS authentication scheme, RADIUS authorization will fail.

Related commands: **authorization default**, **hwtacacs scheme**, **radius scheme**.

Examples

Configure the default ISP domain **system** to use local authorization for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization login local
```

Configure the default ISP domain **system** to use RADIUS authorization scheme **rd** for login users and use local authorization as the backup.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization login radius-scheme rd local
```

authorization-attribute

Syntax

authorization-attribute { **acl** *acl-number* | **callback-number** *callback-number* | **idle-cut** *minute* | **level** *level* | **user-profile** *profile-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *

undo authorization-attribute { **acl** | **callback-number** | **idle-cut** | **level** | **user-profile** | **vlan** | **work-directory** } *

View

Local user view, user group view

Default Level

3: Manage level

Parameters

acl: Specifies the authorized ACL of the local user(s).

acl-number: Authorized ACL for the local user(s), in the range 2000 to 5999.

callback-number: Specifies the authorization PPP callback number of the local user(s).

callback-number: Authorization PPP callback number for the local user(s), a case-sensitive string of 1 to 64 characters.

idle-cut: Specifies the idle cut function for the local user(s). With the idle cut function enabled, an online user whose idle period exceeds the specified idle time will be logged out.

minute: Idle time allowed, in the range 1 to 120 minutes.

level: Specifies the level of the local user(s).

level: Level of the local user(s), which can be 0 for visit level, 1 for monitor level, 2 for system level, and 3 for manage level. A smaller number means a lower level. The default is 0.

user-profile: Specifies the authorization user profile of the local user(s).

profile-name: Name of the authorization user profile for the local user(s), a case-sensitive string of 1 to 32 characters. It can consist of English letters, digits, and underlines and must start with an English letter.

vlan: Specifies the authorized VLAN of the local user(s).

vlan-id: Authorized VLAN for the local user(s), in the range 1 to 4094.

work-directory: Specifies the authorized work directory of the local user(s), if the user or users are authorized the FTP or SFTP service type.

directory-name: Authorized work directory, a case-insensitive string of 1 to 135 characters. This directory must already exist.

Description

Use the **authorization-attribute** command to configure authorization attributes for the local user or user group. After the local user or a local user of the user group passes authentication, the device will assign these attributes to the user.

Use the **undo authorization-attribute** command to remove authorization attributes.

By default, no authorization attribute is configured for a local user or user group.

Note that:

- Every configurable authorization attribute has its definite application environments and purposes. However, the assignment of local user authorization attributes does not take the service type into account. Therefore, when configuring authorization attributes for a local user, consider what attributes are needed.
- Authorization attributes configured for a user group are effective on all local users of the group.
- An authorization attribute configured in local user view takes precedence over the same attribute configured in user group view.
- If you specify to perform no authentication or perform password authentication, the levels of commands that a user can access after login depends on the level of the user interface. For information about user interface login authentication method, refer to the **authentication-mode**

command in *Login Commands* of the *System Volume*. If the authentication method requires users to provide usernames and passwords, the levels of commands that a user can access after login depends on the level of the user. For an SSH user authenticated with an RSA public key, available commands depend on the level specified on the user interface.

- If you remove the specified work directory from the file system, the FTP/SFTP user(s) will not be able to access the directory.
- If the specified work directory carries slot information, the FTP/SFTP user(s) will not be able to access the directory after a switchover occurs. Therefore, specifying slot information for the work directory is not recommended.

Examples

Configure the authorized VLAN of user group **abc** as VLAN 3.

```
<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc] authorization-attribute vlan 3
```

bind-attribute

Syntax

bind-attribute { **call-number** *call-number* [**:** *subcall-number*] | **ip** *ip-address* | **location port** *slot-number subslot-number port-number* | **mac** *mac-address* | **vlan** *vlan-id* } *

undo bind-attribute { **call-number**| **ip** | **location** | **mac** | **vlan** } *

View

Local user view

Default Level

3: Manage level

Parameters

call-number *call-number*: Specifies a calling number for ISDN user authentication. The *call-number* argument is a string of 1 to 64 characters.

subcall-number: Specifies the sub-calling number. The total length of the calling number and the sub-calling number cannot be more than 62 characters.

ip *ip-address*: Specifies the IP address of the user.

location: Specifies the port binding attribute of the user.

port *slot-number subslot-number port-number*: Specifies the port to which the user is bound. The *slot-number* argument is in the range 0 to 15, the *subslot-number* argument is in the range 0 to 15, and the *port-number* argument is in the range 0 to 255. Only the numbers make sense here; port types are not taken into account.

mac *mac-address*: Specifies the MAC address of the user in the format of H-H-H.

vlan *vlan-id*: Specifies the VLAN to which the user belongs. The *vlan-id* argument is in the range 1 to 4094.

Description

Use the **bind-attribute** command to configure binding attributes for a local user.

Use the **undo bind-attribute** command to remove binding attributes of a local user.

By default, no binding attribute is configured for a local user.

Note that:

- Binding attributes are checked upon authentication of a local user. If the binding attributes of a local user do not match the configured ones, the checking will fail and the user will fail the authentication as a result. In addition, such binding attribute checking does not take the service types of the users into account. That is, a configured binding attribute is effective on all types of users. Therefore, be cautious when deciding which binding attributes should be configured for which type of local users.
- The **bind-attribute ip** command applies only when the authentication method (802.1X, for example) supports IP address upload. If you configure the command when the authentication method (MAC address authentication, for example) does not support IP address upload, local authentication will fail.
- The **bind-attribute mac** command applies to only LAN users, for example, 802.1X users. If you configure it for other types of users, such as FTP or Telnet users, local authentication of the users will fail.

Examples

Configure the bound IP of local user **abc** as 3.3.3.3.

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] bind-attribute ip 3.3.3.3
```

cut connection

Syntax

cut connection { **access-type** { **dot1x** | **mac-authentication** } | **all** | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id* } [**slot** *slot-number*]

View

System view

Default Level

2: System level

Parameters

access-type: Specifies user connections of an access mode.

- **dot1x**: Specifies 802.1x authentication user connections.
- **mac-authentication**: Specifies MAC authentication user connections.

all: Specifies all user connections.

domain *isp-name*: Specifies all user connections of an ISP domain. The *isp-name* argument refers to the name of an existing ISP domain and is a string of 1 to 24 characters.

interface *interface-type interface-number*: Specifies all user connections of an interface.

ip *ip-address*: Specifies a user connection by IP address.

mac *mac-address*: Specifies a user connection by MAC address. The MAC address must be in the format of *H-H-H.*

ucibindex *ucib-index*: Specifies a user connection by connection index. The value ranges from 0 to 4294967295.

user-name *user-name*: Specifies a user connection by username. The *user-name* argument is a case-sensitive string of 1 to 80 characters and must contain the domain name. If you enter a username without any domain name, the system assumes that the default domain name is used for the username.

slot *slot-number*: Specifies the connections on a specified member device in an IRF. The *slot-number* argument indicates the member device ID.

Description

Use the **cut connection** command to tear down the specified connections forcibly.

At present, this command applies to only LAN access user connections.

Related commands: **display connection**, **service-type**.

Examples

Tear down all connections in ISP domain **aabbcc.net.**

```
<Sysname> system-view
[Sysname] cut connection domain aabbcc.net
```

display connection

Syntax

display connection [**access-type** { **dot1x** | **mac-authentication** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id*] [**slot** *slot-number*]

View

Any view

Default Level

1: Monitor level

Parameters

access-type: Specifies user connections of an access mode.

- **dot1x**: Specifies 802.1x authentication user connections.
- **mac-authentication**: Specifies MAC authentication user connections.

domain *isp-name*: Specifies all user connections of an ISP domain. The *isp-name* argument refers to the name of an existing ISP domain and is a case-insensitive string of 1 to 24 characters.

interface *interface-type interface-number*: Specifies all user connections of an interface.

ip *ip-address*: Specifies a user connection by IP address.

mac *mac-address*: Specifies a user connection by MAC address. The MAC address must be in the format of *H-H-H.*

ucibindex *ucib-index*: Specifies all user connections using the specified connection index. The value ranges from 0 to 4294967295.

user-name *user-name*: Specifies all user connections using the specified username. The *user-name* argument is a case-sensitive string of 1 to 80 characters and must contain the domain name. If you enter a username without any domain name, the system assumes that the default domain name is used for the username.

slot *slot-number*: Specifies the connections on a specified member device in an IRF. The *slot-number* argument indicates the member device ID.

Description

Use the **display connection** command to display information about specified or all AAA user connections.

Note that:

- With no parameter specified, the command displays brief information about all AAA user connections.
- If you specify the **ucibindex** *ucib-index* combination, the command displays detailed information; otherwise, the command displays brief information.
- This command does not apply to FTP user connections.

Related commands: **cut connection**.

Examples

Display information about all AAA user connections.

```
<Sysname> display connection

Index=1   ,Username=telnet@system
IP=10.0.0.1
 Total 1 connection(s) matched.
```

Table 1-1 display connection command output description

Field	Description
Index	Index number
Username	Username of the connection, in the format *username@domain*
IP	IP address of the user
Total 1 connection(s) matched.	Total number of user connections

display domain

Syntax

display domain [*isp-name*]

View

Any view

Default Level

1: Monitor level

Parameters

isp-name: Name of an existing ISP domain, a string of 1 to 24 characters.

Description

Use the **display domain** command to display the configuration information of a specified ISP domain or all ISP domains.

Related commands: **access-limit enable**, **domain**, **state**.

Examples

Display the configuration information of all ISP domains.

```
<Sysname> display domain
0  Domain = system
   State = Active
   Access-limit = Disable
   Accounting method = Required
   Default authentication scheme     : local
   Default authorization scheme      : local
   Default accounting scheme         : local
   Domain User Template:
   Idle-cut = Disabled
   Self-service = Disabled

1  Domain = aabbcc
   State = Active
   Access-limit = Disable
   Accounting method = Required
   Default authentication scheme     : local
   Default authorization scheme      : local
   Default accounting scheme         : local
   Lan-access authentication scheme   : radius=test, local
   Lan-access authorization scheme    : hwtacacs=hw, local
   Lan-access accounting scheme      : local
   Domain User Template:
   Idle-cut = Disabled
   Self-service = Disabled


Default Domain Name: system
Total 2 domain(s)
```

Table 1-2 display domain command output description

Field	Description
Domain	Domain name

Field	Description
State	Status of the domain (active or block)
Access-limit	Limit on the number of user connections
Accounting method	Accounting method (either required or optional)
Default authentication scheme	Default authentication method
Default authorization scheme	Default authorization method
Default accounting scheme	Default accounting method
Lan-access authentication scheme	Authentication method for LAN users
Lan-access authorization scheme	Authentication method for LAN users
Lan-access accounting scheme	Accounting method for LAN users
Domain User Template	Template for users in the domain
Idle-cut	Whether idle cut is enabled
Self-service	Whether self service is enabled
Default Domain Name	Default ISP domain name
Total 2 domain(s).	2 ISP domains in total

display local-user

Syntax

display local-user [**idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** *vlan-id*] [**slot** *slot-number*]

View

Any view

Default Level

1: Monitor level

Parameters

idle-cut { **disable** | **enable** }: Specifies local users with the idle cut function disabled or enabled.

service-type: Specifies the local users of a type.

- **ftp** refers to users using FTP.
- **lan-access** refers to users accessing the network through an Ethernet, such as 802.1X users.
- **ssh** refers to users using SSH.
- **telnet** refers to users using Telnet.
- terminal refers to users logging in through the console port or AUX port.
- **state** { **active** | **block** }: Specifies all local users in the state of active or block. A local user in the state of active can access network services, while a local user in the state of blocked cannot.

user-name *user-name*: Specifies all local users using the specified username. The username is a case-sensitive string of 1 to 55 characters and does not contain the domain name.

vlan *vlan-id*: Specifies all local users in a VLAN. The VLAN ID ranges from 1 to 4094.

slot *slot-number*: Specifies all local users on a specified member device in an IRF. The *slot-number* argument indicates the member device ID.

Description

Use the **display local-user** command to display information about specified or all local users.

Related commands: **local-user**.

Examples

Display the information of local user **bbb** on the specified Unit ID.

```
<Sysname> display local-user user-name bbb slot 1
Slot:  1
The contents of local user bbb:
 State:                    Active
 ServiceType:               ftp
 Access-limit:              Enable          Current AccessNum: 0
 Max AccessNum:             300
 User-group:                system
 Bind attributes:
  IP address:               1.2.3.4
  Bind location:            0/4/1 (SLOT/SUBSLOT/PORT)
  MAC address:              0001-0002-0003
  Vlan ID:                  100
 Authorization attributes:
  Idle TimeOut:             10(min)
  Work Directory:           flash:/
  User Privilege:           3
  Acl ID:                   2000
  Vlan ID:                  100
  User Profile:             prof1
 Expiration date:           12:12:12-2018/09/16
Total 1 local user(s) matched.
```

Table 1-3 display local-user command output description

Field	Description
Slot	Slot number of the card
State	Status of the local user, Active or Block
ServiceType	Service types that the local user can use, including FTP, LAN, SSH, Telnet, and terminal.
Access-limit	Limit on the number of user connections using the current username
Current AccessNum	Current number of user connections using the current username, either for all cards or for a specified card.
Max AccessNum	Maximum number of user connections using the current username
VLAN ID	VLAN to which the user is bound
Calling Number	Calling number of the ISDN user

Field	Description
Authorization attributes	Authorization attributes of the local user
Idle TimeOut	Idle threshold of the user, in minutes.
Callback-number	Authorized PPP callback number of the local user
Work Directory	Directory accessible to the FTP user
VLAN ID	Authorized VLAN of the local user
Expiration date	Expiration time of the local user

display user-group

Syntax

display user-group [*group-name*]

View

Any view

Default Level

2: System level

Parameters

group-name: User group name, a case-insensitive string of 1 to 32 characters.

Description

Use the **display user-group** command to display configuration information about one or all user groups.

Related commands: **user-group**.

Examples

Display configuration information about user group **abc**.

```
<Sysname> display user-group abc
The contents of user group abc:
 Authorization attributes:
  Idle-cut:              120(min)
  Work Directory:         FLASH:
  Level:                1
  Acl Number:            2000
  Vlan ID:              1
  User-Profile:          1
  Callback-number:        1
Total 1 user group(s) matched.
```

domain

Syntax

domain *isp-name*

undo domain *isp-name*

View

System view

Default Level

3: Manage level

Parameters

isp-name: ISP domain name, a case-insensitive string of 1 to 24 characters that cannot contain any forward slash (/), colon (:), asterisk (*), question mark (?), less-than sign (<), greater-than sign (>), or @.

Description

Use the **domain** *isp-name* command to create an ISP domain and/or enter ISP domain view.

Use the **undo domain** command to remove an ISP domain.

Note that:

- If the specified ISP domain does not exist, the system will create a new ISP domain. All the ISP domains are in the active state when they are created.
- There is a default domain in the system, which cannot be deleted and can only be changed. A user providing no ISP domain name is considered in the default domain. For details about the default domain, refer to command **domain default enable**.

Related commands: **state**, **display domain**.

Examples

Create ISP domain **aabbcc.net**, and enter ISP domain view.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net]
```

domain default enable

Syntax

domain default enable *isp-name*

undo domain default enable

View

System view

Default Level

3: Manage level

Parameters

isp-name: Name of the default ISP domain, a string of 1 to 24 characters.

Description

Use the **domain default enable** command to configure the system default ISP domain.

Use the **undo domain default enable** command to restore the default.

By default, there is a default ISP domain named **system**.

Note that:

- There must be only one default ISP domain.
- The specified domain must have existed; otherwise, users without any domain name carried in the user name will fail to be authenticated.
- The default ISP domain configured cannot be deleted unless you configure it as a non-default domain again.

Related commands: **state**, **display domain**.

Examples

Create a new ISP domain named **aabbcc.net**, and configure it as the default ISP domain.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] quit
[Sysname] domain default enable aabbcc.net
```

expiration-date

Syntax

expiration-date *time*

undo expiration-date

View

Local user view

Default Level

3: Manage level

Parameters

time: Expiration time of the local user, in the format HH:MM:SS-MM/DD/YYYY or HH:MM:SS-YYYY/MM/DD. HH:MM:SS indicates the time, where HH ranges from 0 to 23, MM and SS range from 0 to 59. YYYY/MM/DD indicates the date, where YYYY ranges from 2000 to 2035, MM ranges from 1 to 12, and DD depends on the month. Except for the zeros in 00:00:00, leading zeros can be omitted. For example, 2:2:0-2008/2/2 equals to 02:02:00-2008/02/02.

Description

Use the **expiration-date** command to configure the expiration time of a local user.

Use the **undo expiration-date** command to remove the configuration.

By default, a local user has no expiration time and no time validity checking is performed.

When some users need to access the network temporarily, you can create a guest account and specify an expiration time for the account. When a user uses the guest account for local authentication and passes the authentication, the access device checks whether the current system time is within the expiration time. If so, it permits the user to access the network. Otherwise, it denies the access request of the user.

Note that if you change the system time manually or the system time is changed in any other way, the access device uses the new system time for time validity checking.

Examples

Configure the expiration time of user **abc** to be 12:10:20 on May 31, 2008.

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] expiration-date 12:10:20-2008/05/31
```

group

Syntax

group *group-name*

undo group

View

Local user view

Default Level

3: Manage level

Parameters

group-name: User group name, a case-insensitive string of 1 to 32 characters.

Description

Use the **group** command to specify the user group for the local user to belong to.

Use the **undo group** command to restore the default.

By default, a local user belongs to user group **system**, which is automatically created by the device.

Examples

Specify that local user 111 belongs to user group **abc**.

```
<Sysname> system-view
[Sysname] local-user 111
[Sysname-luser-111] group abc
```

idle-cut enable

Syntax

idle-cut enable *minute*

undo idle-cut enable

View

ISP domain view

Default Level

2: System level

Parameters

minute: Maximum idle duration allowed, in the range 1 to 120 minutes.

Description

Use the **idle-cut enable** command to enable the idle cut function and set the maximum idle duration allowed. With the idle cut function enabled for a domain, the system will log out any user in the domain who has been idle for a period greater than the maximum idle duration.

Use the **undo idle-cut** command to restore the default.

By default, the function is disabled.

Related commands: **domain**.

Examples

Enable the idle cut function and set the idle threshold to 50 minutes for ISP domain **aabbcc.net**.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] idle-cut enable 50
```

local-user

Syntax

local-user *user-name*

undo local-user { *user-name* | **all service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** } }

View

System view

Default Level

3: Manage level

Parameters

user-name: Name for the local user, a case-sensitive string of 1 to 55 characters that does not contain the domain name. It cannot contain any backward slash (\), forward slash (/), vertical line (|), colon (:), asterisk (*), question mark (?), less-than sign (<), greater-than sign (>) and the @ sign and cannot be a, al, or all.

all: Specifies all users.

service-type: Specifies the users of a type.

- **ftp** refers to users using FTP.
- **lan-access** refers to users accessing the network through an Ethernet, such as 802.1X users.
- **ssh** refers to users using SSH.

- **telnet** refers to users using Telnet.
- **terminal** refers to users logging in through the console port or AUX port.

Description

Use the **local-user** command to add a local user and enter local user view.

Use the **undo local-user** command to remove the specified local users.

By default, no local user is configured.

Related commands: **display local-user**, **service-type**.

Examples

Add a local user named **user1**.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1]
```

local-user password-display-mode

Syntax

local-user password-display-mode { **auto** | **cipher-force** }

undo local-user password-display-mode

View

System view

Default Level

2: System level

Parameters

auto: Displays the password of a user based on the configuration of the user by using the **password** command.

cipher-force: Displays the passwords of all users in cipher text.

Description

Use the **local-user password-display-mode** command to set the password display mode for all local users.

Use the **undo local-user password-display-mode** command to restore the default.

The default mode is **auto**.

With the **cipher-force** mode configured:

- A local user password is always displayed in cipher text, regardless of the configuration of the **password** command.
- If you use the **save** command to save the configuration, all existing local user passwords will still be displayed in cipher text after the device restarts, even if you restore the display mode to **auto**.

Related commands: **display local-user**, **password**.

Examples

Specify to display the passwords of all users in cipher text.

```
<Sysname> system-view
[Sysname] local-user password-display-mode cipher-force
```

password

Syntax

password { **cipher** | **simple** } *password*

undo password

View

Local user view

Default Level

2: System level

Parameters

cipher: Specifies to display the password in cipher text.

simple: Specifies to display the password in simple text.

password: Password for the local user.

- In simple text, it must be a string of 1 to 63 characters that contains no blank space, for example, aabbcc.
- In cipher text, it must be a string of 24 or 88 characters, for example, _(TT8F]Y\5SQ=^Q`MAF4<1!!.
- With the **simple** keyword, you must specify the password in simple text. With the **cipher** keyword, you can specify the password in either simple or cipher text.

Description

Use the **password** command to configure a password for a local user.

Use the **undo password** command to delete the password of a local user.

Note that:

- With the **local-user password-display-mode cipher-force** command configured, the password is always displayed in cipher text, regardless of the configuration of the **password** command.
- With the **cipher** keyword specified, a password of up to 16 characters in plain text will be encrypted into a password of 24 characters in cipher text, and a password of 16 to 63 characters in plain text will be encrypted into a password of 88 characters in cipher text. For a password of 24 characters, if the system can decrypt the password, the system treats it as a password in cipher text. Otherwise, the system treats it as a password in plain text.

Related commands: **display local-user**.

Examples

Set the password of **user1** to 123456 and specify to display the password in plain text.

```
<Sysname> system-view
[Sysname] local-user user1
```

```
[Sysname-luser-user1] password simple 123456
```

self-service-url enable

Syntax

self-service-url enable *url-string*

undo self-service-url enable

View

ISP domain view

Default Level

2: System level

Parameters

url-string: URL of the self-service server for changing user password, a string of 1 to 64 characters. It must start with http:// and contain no question mark.

Description

Use the **self-service-url enable** command to enable the self-service server localization function and specify the URL of the self-service server for changing user password.

Use the **undo self-service-url enable** command to restore the default.

By default, the function is disabled.

Note that:

- A self-service RADIUS server, for example, iMC, is required for the self-service server localization function. With the self-service function, a user can manage and control his or her accounting information or card number. A server with self-service software is a self-service server.
- After you configure the **self-service-url enable** command, a user can locate the self-service server by selecting [Service/Change Password] from the 802.1X client. The client software automatically launches the default browser, IE or Netscape, and opens the URL page of the self-service server for changing the user password. A user can change his or her password through the page.
- Only authenticated users can select [Service/Change Password] from the 802.1X client. The option is gray and unavailable for unauthenticated users.

Examples

Enable the self-service server localization function and specify the URL of the self-service server for changing user password to http://10.153.89.94/selfservice/modPasswd1x.jsp|userName for the default ISP domain **system**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system]                    self-service-url                    enable
http://10.153.89.94/selfservice/modPasswd1x.jsp|userName
```

service-type

Syntax

service-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** } * }

undo service-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** } * }

View

Local user view

Default Level

3: Manage level

Parameters

ftp: Authorizes the user to use the FTP service. The user can use the root directory of the FTP server by default.

lan-access: Authorizes the user to use the LAN access service. Such users are mainly Ethernet users, for example, 802.1X users.

ssh: Authorizes the user to use the SSH service.

telnet: Authorizes the user to use the Telnet service.

terminal: Authorizes the user to use the terminal service, allowing the user to login from the console port or AUX port.

Description

Use the **service-type** command to specify the service types that a user can use.

Use the **undo service-type** command to delete one or all service types configured for a user.

By default, a user is authorized with no service.

Examples

Authorize user **user1** to use the Telnet service.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] service-type telnet
```

state

Syntax

state { **active** | **block** }

undo state

View

ISP domain view, local user view

Default Level

2: System level

Parameters

active: Places the current ISP domain or local user in the active state, allowing the users in the current ISP domain or the current local user to request network services.

block: Places the current ISP domain or local user in the blocked state, preventing users in the current ISP domain or the current local user from requesting network services.

Description

Use the **state** command to configure the status of the current ISP domain or local user.

Use the **undo state** command to restore the default.

By default, an ISP domain is active when created. So is a local user.

By blocking an ISP domain, you disable users of the domain that are offline from requesting network services. Note that the online users are not affected.

By blocking a user, you disable the user from requesting network services. No other users are affected.

Related commands: **domain**.

Examples

Place the current ISP domain **aabbcc.net** to the state of blocked.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] state block
```

Place the current user **user1** to the state of blocked.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-user-user1] state block
```

user-group

Syntax

user-group *group-name*

undo user-group *group-name*

View

System view

Default Level

3: Manage level

Parameters

group-name: User group name, a case-insensitive string of 1 to 32 characters.

Description

Use the **user-group** command to create a user group and enter its view.

Use the **undo user-group** command to remove a user group.

A user group consists of a group of local users and has a set of local user attributes. You can configure local user attributes for a user group to implement centralized management of user attributes for the local users in the group. Currently, you can configure authorization attributes for a user group.

Note that:

- A user group with one or more local users cannot be removed.
- The default system user group **system** cannot be removed but you can change its configurations.

Related commands: **display user-group**.

Examples

Create a user group named **abc** and enter its view.

```
<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc]
```

2 RADIUS Configuration Commands

RADIUS Configuration Commands

data-flow-format (RADIUS scheme view)

Syntax

data-flow-format { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } } *

undo data-flow-format { **data** | **packet** }

View

RADIUS scheme view

Default Level

2: System level

Parameters

data: Specifies the unit for data flows, which can be byte, kilobyte, megabyte, or gigabyte.

packet: Specifies the unit for data packets, which can be one-packet, kilo-packet, mega-packet, or giga-packet.

Description

Use the **data-flow-format** command to specify the unit for data flows or packets to be sent to a RADIUS server.

Use the **undo data-flow-format** command to restore the default.

By default, the unit for data flows is **byte** and that for data packets is **one-packet**.

Note that:

- The specified unit of data flows sent to the RADIUS server must be consistent with the traffic statistics unit of the RADIUS server. Otherwise, accounting cannot be performed correctly.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **display radius scheme**.

Examples

Define RADIUS scheme **radius1** to send data flows and packets destined for the RADIUS server in kilobytes and kilo-packets.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] data-flow-format data kilo-byte packet kilo-packet
```

display radius scheme

Syntax

display radius scheme [*radius-scheme-name*] [**slot** *slot-number*]

View

Any view

Default Level

2: System level

Parameters

radius-scheme-name: RADIUS scheme name.

slot *slot-number*: Specifies the specified member device in an IRF. The *slot-number* argument indicates the member device ID.

Description

Use the **display radius scheme** command to display the configuration information of a specified RADIUS scheme or all RADIUS schemes.

Note that:

- If no RADIUS scheme is specified, the command will display the configurations of all RADIUS schemes.
- If no slot number is specified, the command will display the configurations of the RADIUS schemes on only the specified member device.

Related commands: **radius scheme**.

Examples

Display the configurations of all RADIUS schemes.

```
<Sysname> display radius scheme
------------------------------------------------------------------
  SchemeName  : radius1
  Index : 0                       Type : extended
  Primary Auth IP  : 1.1.1.1        Port : 1812   State : active
  Primary Acct IP  : 1.1.1.1        Port : 1813   State : active
  Second  Auth IP  : 0.0.0.0        Port : 1812   State : block
  Second  Acct IP  : 0.0.0.0        Port : 1813   State : block
  Auth Server Encryption Key : 123
  Acct Server Encryption Key : Not configured
  Interval for timeout(second)                      : 3
  Retransmission times for timeout                  : 3
  Interval for realtime accounting(minute)          : 12
  Retransmission times of realtime-accounting packet    : 5
  Retransmission times of stop-accounting packet        : 500
  Quiet-interval(min)                               : 5
  Username format                                   : without-domain
  Data flow unit                                    : Byte
```

```
  Packet unit                                 : one

------------------------------------------------------------------
Total 1 RADIUS scheme(s)
```

Table 2-1 display radius scheme command output description

Field	Description
SchemeName	Name of the RADIUS scheme
Index	Index number of the RADIUS scheme
Type	Type of the RADIUS server
Primary Auth IP/ Port/ State	IP address/access port number/current status of the primary authentication server: (active or block) If there is no primary authentication server specified, the IP address is 0.0.0.0 and the port number is the default. This rule is also applicable to the following three fields.
Primary Acct IP/ Port/ State	IP address/access port number/current status of the primary accounting server: (active or block)
Second Auth IP/ Port/ State	IP address/access port number/current status of the secondary authentication server: (active or block)
Second Acct IP/ Port/ State	IP address/access port number/current status of the secondary accounting server: (active or block)
Auth Server Encryption Key	Shared key of the authentication server
Acct Server Encryption Key	Shared key of the accounting server
Accounting-On packet disable	The accounting-on function is disabled
send times	Retransmission times of accounting-on packets
interval	Interval to retransmit accounting-on packets
Interval for timeout(second)	Timeout time in seconds
Retransmission times for timeout	Times of retransmission in case of timeout
Interval for realtime accounting(minute)	Interval for realtime accounting in minutes
Retransmission times of realtime-accounting packet	Retransmission times of realtime-accounting packet
Retransmission times of stop-accounting packet	Retransmission times of stop-accounting packet
Quiet-interval(min)	Quiet interval for the primary server
Username format	Format of the username
Data flow unit	Unit of data flows
Packet unit	Unit of packets
Total 1 RADIUS scheme(s)	1 RADIUS scheme in total

display radius statistics

Syntax

display radius statistics [**slot** *slot-number*]

View

Any view

Default Level

2: System level

Parameters

slot *slot-number*: Specifies the specified member device in an IRF. The *slot-number* argument indicates the member device ID.

Description

Use the **display radius statistics** command to display statistics about RADIUS packets.

Related commands: **radius scheme**.

Examples

Display statistics about RADIUS packets on the interface board in slot 1.

```
<Sysname> display radius statistics slot 1
 Slot  1:state statistic(total=4096):
    DEAD = 4096    AuthProc = 0       AuthSucc = 0
AcctStart = 0       RLTSend = 0       RLTWait = 0
 AcctStop = 0        OnLine = 0          Stop = 0
 StateErr = 0

Received and Sent packets statistic:
Sent PKT total   = 1547    Received PKT total = 23
Resend Times    Resend total
1             508
2             508
Total          1016
RADIUS received packets statistic:
Code =  2   Num = 15      Err = 0
Code =  3   Num = 4       Err = 0
Code =  5   Num = 4       Err = 0
Code = 11   Num = 0       Err = 0

Running statistic:
RADIUS received messages statistic:
Normal auth request     Num = 24      Err = 0       Succ = 24
EAP auth request        Num = 0       Err = 0       Succ = 0
Account request         Num = 4       Err = 0       Succ = 4
Account off request     Num = 503     Err = 0       Succ = 503
PKT auth timeout        Num = 15      Err = 5       Succ = 10
```

```
PKT acct_timeout        Num = 1509    Err = 503     Succ = 1006
Realtime Account timer   Num = 0       Err = 0       Succ = 0
PKT response           Num = 23      Err = 0       Succ = 23
Session ctrl pkt        Num = 0       Err = 0       Succ = 0
Normal author request    Num = 0       Err = 0       Succ = 0
Set policy result       Num = 0       Err = 0       Succ = 0
RADIUS sent messages statistic:
Auth accept            Num = 10
Auth reject            Num = 14
EAP auth replying       Num = 0
Account success         Num = 4
Account failure         Num = 3
Server ctrl req         Num = 0
RecError_MSG_sum = 0
SndMSG_Fail_sum  = 0
Timer_Err       = 0
Alloc_Mem_Err    = 0
State Mismatch   = 0
Other_Error     = 0

No-response-acct-stop packet = 1
Discarded No-response-acct-stop packet for buffer overflow = 0
```

Table 2-2 display radius statistics command output description

Field	Description
slot	The specified member device in an IRF. The *slot* indicates the member device ID.
state statistic	state statistics
DEAD	Number of idle users
AuthProc	Number of users waiting for authentication
AuthSucc	Number of users who have passed authentication
AcctStart	Number of users for whom accounting has been started
RLTSend	Number of users for whom the system sends real-time accounting packets
RLTWait	Number of users waiting for real-time accounting
AcctStop	Number of users in the state of accounting waiting stopped
OnLine	Number of online users
Stop	Number of users in the state of stop
StateErr	Number of users with unknown errors
Received and Sent packets statistic	Statistics of packets received and sent
Sent PKT total	Number of packets sent
Received PKT total	Number of packets received
Resend Times	Number of retransmission attempts

Field	Description
Resend total	Number of packets retransmitted
Total	Total number of packets retransmitted
RADIUS received packets statistic	Statistics of packets received by RADIUS
Code	Packet type
Num	Total number of packets
Err	Number of error packets
Running statistic	RADIUS operation message statistics
RADIUS received messages statistic	Number of messages received by RADIUS
Normal auth request	Number of normal authentication requests
EAP auth request	Number of EAP authentication requests
Account request	Number of accounting requests
Account off request	Number of stop-accounting requests
PKT auth timeout	Number of authentication timeout messages
PKT acct_timeout	Number of accounting timeout messages
Realtime Account timer	Number of realtime accounting requests
PKT response	Number of responses
Session ctrl pkt	Number of session control messages
Normal author request	Number of normal authorization requests
Succ	Number of acknowledgement messages
Set policy result	Number of responses to the Set policy packets
RADIUS sent messages statistic	Number of messages that have been sent by RADIUS
Auth accept	Number of accepted authentication packets
Auth reject	Number of rejected authentication packets
EAP auth replying	Number of replying packets of EAP authentication
Account success	Number of accounting succeeded packets
Account failure	Number of accounting failed packets
Server ctrl req	Number of server control requests
RecError_MSG_sum	Number of received packets in error
SndMSG_Fail_sum	Number of packets that failed to be sent out
Timer_Err	Number of timer errors
Alloc_Mem_Err	Number of memory errors
State Mismatch	Number of errors for mismatching status
Other_Error	Number of errors of other types
No-response-acct-stop packet	Number of times that no response was received for stop-accounting packets

Field	Description
Discarded No-response-acct-stop packet for buffer overflow	Number of stop-accounting packets that were buffered but then discarded due to full memory

display stop-accounting-buffer

Syntax

display stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [**slot** *slot-number*]

View

Any view

Default Level

2: System level

Parameters

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

session-id *session-id*: Specifies a session by its ID. The ID is a string of 1 to 50 characters.

time-range *start-time stop-time*: Specifies a time range by its start time and end time in the format of hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd.

user-name *user-name*: Specifies a user by the user name, which is a case-sensitive string of 1 to 80 characters. Whether the *user-name* argument should include the domain name depends on the setting by the **user-name-format** command for the RADIUS scheme.

slot *slot-number*: Specifies the specified member device in an IRF. The *slot-number* argument indicates the member device ID.

Description

Use the **display stop-accounting-buffer** command to display information about the stop-accounting requests buffered in the device by scheme, session ID, time range, user name, or slot.

Note that if receiving no response after sending a stop-accounting request to a RADIUS server, the device buffers the request and retransmits it. You can use the **retry stop-accounting** command to set the number of allowed transmission attempts.

Related commands: **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, **user-name-format**, **retry stop-accounting**.

Examples

Display information about the buffered stop-accounting requests from 0:0:0 to 23:59:59 on August 31, 2006.

```
<Sysname> display stop-accounting-buffer time-range 0:0:0-08/31/2006 23:59:59-08/31/2006
Total 0 record(s) Matched
```

key (RADIUS scheme view)

Syntax

key { **accounting** | **authentication** } *string*

undo key { **accounting** | **authentication** }

View

RADIUS scheme view

Default Level

2: System level

Parameters

accounting: Sets the shared key for RADIUS accounting packets.

authentication: Sets the shared key for RADIUS authentication/authorization packets.

string: Shared key, a case-sensitive string of 1 to 64 characters.

Description

Use the **key** command to set the shared key for RADIUS authentication/authorization or accounting packets.

Use the **undo key** command to restore the default.

By default, no shared key is configured.

Note that:

- You must ensure that the same shared key is set on the device and the RADIUS server.
- If authentication/authorization and accounting are performed on two servers with different shared keys, you must set separate shared key for each on the device.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **display radius scheme**.

Examples

Set the shared key for authentication/authorization packets to hello for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key authentication hello
```

Set the shared key for accounting packets to ok for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting ok
```

nas-ip (RADIUS scheme view)

Syntax

nas-ip *ip-address*

undo nas-ip

View

RADIUS scheme view

Default Level

2: System level

Parameters

ip-address: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

Description

Use the **nas-ip** command to set the IP address for the device to use as the source address of the RADIUS packets to be sent to the server.

Use the **undo nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is that configured by the **radius nas-ip** command in system view.

Note that:

- Specifying a source address for the RADIUS packets to be sent to the server can avoid the situation where the packets sent back by the RADIUS server cannot reach the device as the result of a physical interface failure. The address of a loopback interface is recommended.
- The **nas-ip** command in RADIUS scheme view is only for the current RADIUS scheme, while the **radius nas-ip** command in system view is for all RADIUS schemes. However, the **nas-ip** command in RADIUS scheme view overwrites the configuration of the **radius nas-ip** command.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **radius nas-ip**.

Examples

Set the IP address for the device to use as the source address of the RADIUS packets to 10.1.1.1.

```
<Sysname> system-view
[Sysname] radius scheme test1
[Sysname-radius-test1] nas-ip 10.1.1.1
```

primary accounting (RADIUS scheme view)

Syntax

primary accounting *ip-address* [*port-number*]

undo primary accounting

View

RADIUS scheme view

Default Level

2: System level

Parameters

ip-address: IP address of the primary accounting server.

port-number: UDP port number of the primary accounting server, which ranges from 1 to 65535 and defaults to 1813.

Description

Use the **primary accounting** command to specify the primary RADIUS accounting server.

Use the **undo primary accounting** command to remove the configuration.

By default, no primary RADIUS accounting server is specified.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The RADIUS service port configured on the device and that of the RADIUS server must be consistent.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **key**, **radius scheme**, **state**.

Examples

Specify the IP address of the primary accounting server for RADIUS scheme **radius1** as 10.110.1.2 and the UDP port of the server as 1813.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813
```

primary authentication (RADIUS scheme view)

Syntax

primary authentication *ip-address* [*port-number*]

undo primary authentication

View

RADIUS scheme view

Default Level

2: System level

Parameters

ip-address: IP address of the primary authentication/authorization server.

port-number: UDP port number of the primary authentication/authorization server, which ranges from 1 to 65535 and defaults to 1812.

Description

Use the **primary authentication** command to specify the primary RADIUS authentication/authorization server.

Use the **undo primary authentication** command to remove the configuration.

By default, no primary RADIUS authentication/authorization server is specified.

Note that:

- After creating a RADIUS scheme, you are supposed to configure the IP address and UDP port of each RADIUS server (primary/secondary authentication/authorization or accounting server). Ensure that at least one authentication/authorization server and one accounting server are configured, and that the RADIUS service port settings on the device are consistent with the port settings on the RADIUS servers.
- The IP addresses of the primary and secondary authentication/authorization servers cannot be the same. Otherwise, the configuration fails.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **key**, **radius scheme**, **state**.

Examples

Specify the primary authentication/authorization server for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812
```

radius client

Syntax

radius client enable

undo radius client

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **radius client enable** command to enable the listening port of the RADIUS client.

Use the **undo radius client** command to disable the listening port of the RADIUS client.

By default, the listening port is enabled.

Note that when the listening port of the RADIUS client is disabled:

- The RADIUS client can either accept authentication, authorization or accounting requests or process timer messages. However, it fails to transmit and receive packets to and from the RADIUS server.

- The end account packets of online users cannot be sent out and buffered. This may cause a problem that the RADIUS server still has the user record after a user goes offline for a period of time.
- The authentication, authorization and accounting turn to the local scheme after the RADIUS request fails if the RADIUS scheme and the local authentication, authorization and accounting scheme are configured.
- The buffered accounting packets cannot be sent out and will be deleted from the buffer when the configured maximum number of attempts is reached.

Examples

Enable the listening port of the RADIUS client.

```
<Sysname> system-view
[Sysname] radius client enable
```

radius nas-ip

Syntax

radius nas-ip *ip-address*

undo radius nas-ip

View

System view

Default Level

2: System level

Parameters

ip-address: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

Description

Use the **radius nas-ip** command to set the IP address for the device to use as the source address of the RADIUS packets to be sent to the server.

Use the **undo radius nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the RADIUS packets to be sent to the server can avoid the situation where the packets sent back by the RADIUS server cannot reach the device as the result of a physical interface failure.
- If you configure the command for more than one time, the last configuration takes effect.
- The **nas-ip** command in RADIUS scheme view is only for the current RADIUS scheme, while the **radius nas-ip** command in system view is for all RADIUS schemes. However, the **nas-ip** command in RADIUS scheme view overwrites the configuration of the **radius nas-ip** command.

Related commands: **nas-ip**.

Examples

Set the IP address for the device to use as the source address of the RADIUS packets to 129.10.10.1.

```
<Sysname> system-view
[Sysname] radius nas-ip 129.10.10.1
```

radius scheme

Syntax

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

View

System view

Default Level

3: Manage level

Parameters

radius-scheme-name: RADIUS scheme name, a case-insensitive string of 1 to 32 characters.

Description

Use the **radius scheme** command to create a RADIUS scheme and enter RADIUS scheme view.

Use the **undo radius scheme** command to delete a RADIUS scheme.

By default, no RADIUS scheme is defined.

Note that:

- The RADIUS protocol is configured scheme by scheme. Every RADIUS scheme must at least specify the IP addresses and UDP ports of the RADIUS authentication/authorization/accounting servers and the parameters necessary for a RADIUS client to interact with the servers.
- A RADIUS scheme can be referenced by more than one ISP domain at the same time.
- You cannot remove the RADIUS scheme being used by online users with the **undo radius scheme** command.

Related commands: **key**, **retry realtime-accounting**, **timer realtime-accounting**, **stop-accounting-buffer enable**, **retry stop-accounting**, **server-type**, **state**, **user-name-format**, **retry**, **display radius scheme**, **display radius statistics**.

Examples

Create a RADIUS scheme named **radius1** and enter RADIUS scheme view.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1]
```

radius trap

Syntax

radius trap { **accounting-server-down** | **authentication-server-down** }

undo radius trap { **accounting-server-down** | **authentication-server-down** }

View

System view

Default Level

2: System level

Parameters

accounting-server-down: RADIUS trap for accounting servers.

authentication-server-down: RADIUS trap for authentication servers.

Description

Use the **radius trap** command to enable the RADIUS trap function.

Use the **undo radius trap** command to disable the function.

By default, the RADIUS trap function is disabled.

Note that:

- If a NAS sends an accounting or authentication request to the RADIUS server but gets no response, the NAS retransmits the request. With the RADIUS trap function enabled, when the NAS transmits the request for half of the specified maximum number of transmission attempts, it sends a trap message; when the NAS transmits the request for the specified maximum number, it sends another trap message.
- If the specified maximum number of transmission attempts is odd, the half of the number refers to the smallest integer greater than the half of the number.

Examples

Enable the RADIUS trap function for accounting servers.

```
<Sysname> system-view
[Sysname] radius trap accounting-server-down
```

reset radius statistics

Syntax

reset radius statistics [**slot** *slot-number*]

View

User view

Default Level

2: System level

Parameters

slot *slot-number*: Specifies the specified member device in an IRF. The *slot-number* argument indicates the member device ID.

Description

Use the **reset radius statistics** command to clear RADIUS statistics.

Related commands: **display radius scheme**.

Examples

Clear RADIUS statistics.

```
<Sysname> reset radius statistics
```

reset stop-accounting-buffer

Syntax

reset stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [**slot** *slot-number*]

View

User view

Default Level

2: System level

Parameters

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, a string of 1 to 32 characters.

session-id *session-id*: Specifies a session by its ID, a string of 1 to 50 characters.

time-range *start-time stop-time*: Specifies a time range by its start time and end time in the format of hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd.

user-name *user-name*: Specifies a user name based on which to reset the stop-accounting buffer. The username is a case-sensitive string of 1 to 80 characters. The format of the *user-name* argument (for example, whether the domain name should be included) must comply with that specified for usernames to be sent to the RADIUS server in the RADIUS scheme.

slot *slot-number*: Specifies the specified member device in an IRF. The *slot-number* argument indicates the member device ID.

Description

Use the **reset stop-accounting-buffer** command to clear the buffered stop-accounting requests, which get no responses.

Related commands: **stop-accounting-buffer enable**, **retry stop-accounting**, **user-name-format**, **display stop-accounting-buffer**.

Examples

Clear the buffered stop-accounting requests for user **user0001@aabbcc.net**.

```
<Sysname> reset stop-accounting-buffer user-name user0001@aabbcc.net
```

Clear the buffered stop-accounting requests in the time range from 0:0:0 to 23:59:59 on August 31, 2006.

```
<Sysname> reset stop-accounting-buffer time-range 0:0:0-08/31/2006 23:59:59-08/31/2006
```

retry

Syntax

retry *retry-times*

undo retry

View

RADIUS scheme view

Default Level

2: System level

Parameters

retry-times: Maximum number of transmission attempts, in the range 1 to 20.

Description

Use the **retry** command to set the maximum number of RADIUS transmission attempts.

Use the **undo retry** command to restore the default.

The default value for the *retry-times* argument is 3.

Note that:

- As RADIUS uses UDP packets to transmit data, the communication is not reliable. If the device does not receive a response to its request from the RADIUS server within the response timeout time, it will retransmit the RADIUS request. If the number of transmission attempts exceeds the limit but the device still receives no response from the RADIUS server, the device regards that the authentication fails.
- The maximum number of transmission attempts defined by this command refers to the sum of all transmission attempts sent by the device to the primary server and the secondary server. For example, assume that the maximum number of transmission attempts is N and both the primary server and secondary RADIUS server are specified and exist, the device will send a request to the other server if the current server does not respond after the sum of transmission attempts reaches N/2 (if N is an even number) or (N+1)/2 (if N is an odd number).
- The maximum number of transmission attempts multiplied by the RADIUS server response timeout period cannot be greater than 75.

Related commands: **radius scheme**, **timer response-timeout**.

Examples

Set the maximum number of RADIUS request transmission attempts to 5 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] retry 5
```

retry realtime-accounting

Syntax

retry realtime-accounting *retry-times*

undo retry realtime-accounting

View

RADIUS scheme view

Default Level

2: System level

Parameters

retry-times: Maximum number of accounting request transmission attempts. It ranges from 1 to 255 and defaults to 5.

Description

Use the **retry realtime-accounting** command to set the maximum number of accounting request transmission attempts.

Use the **undo retry realtime-accounting** command to restore the default.

Note that:

- A RADIUS server usually checks whether a user is online by a timeout timer. If it receives from the NAS no real-time accounting packet for a user in the timeout period, it considers that there may be line or device failure and stops accounting for the user. This may happen when some unexpected failure occurs. In this case, the NAS is required to disconnect the user in accordance. This is done by the maximum number of accounting request transmission attempts. Once the limit is reached but the NAS still receives no response, the NAS disconnects the user.
- Suppose that the RADIUS server response timeout period is 3 seconds (set with the **timer response-timeout** command), the timeout retransmission attempts is 3 (set with the **retry** command), and the real-time accounting interval is 12 minutes (set with the **timer realtime-accounting** command), and the maximum number of accounting request transmission attempts is 5 (set with the **retry realtime-accounting** command). In such a case, the device generates an accounting request every 12 minutes, and retransmits the request when receiving no response within 3 seconds. The accounting is deemed unsuccessful if no response is received within 3 requests. Then the device sends a request every 12 minutes, and if for 5 times it still receives no response, the device will cut the user connection.

Related commands: **radius scheme**, **timer realtime-accounting**.

Examples

Set the maximum number of accounting request transmission attempts to 10 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry realtime-accounting 10
```

retry stop-accounting (RADIUS scheme view)

Syntax

retry stop-accounting *retry-times*

undo retry stop-accounting

View

RADIUS scheme view

Default Level

2: System level

Parameters

retry-times: Maximum number of stop-accounting request transmission attempts. It ranges from 10 to 65,535 and defaults to 500.

Description

Use the **retry stop-accounting** command to set the maximum number of stop-accounting request transmission attempts.

Use the **undo retry stop-accounting** command to restore the default.

- Suppose that the RADIUS server response timeout period is 3 seconds (set with the **timer response-timeout** command), the timeout retransmission attempts is 5 (set with the **retry** command), and the maximum number of stop-accounting request transmission attempts is 20 (set with the **retry stop-accounting** command). This means that for each stop-accounting request, if the device receives no response within 3 seconds, it will initiate a new request. If still no responses are received within 5 renewed requests, the stop-accounting request is deemed unsuccessful. Then the device will temporarily store the request in the device and resend a request and repeat the whole process described above. Only when 20 consecutive attempts fail will the device discard the request.

Related commands: **reset stop-accounting-buffer**, **radius scheme**, **display stop-accounting-buffer**.

Examples

Set the maximum number of stop-accounting request transmission attempts to 1,000 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry stop-accounting 1000
```

secondary accounting (RADIUS scheme view)

Syntax

secondary accounting *ip-address* [*port-number*]

undo secondary accounting

View

RADIUS scheme view

Default Level

2: System level

Parameters

ip-address: IP address of the secondary accounting server, in dotted decimal notation. The default is 0.0.0.0.

port-number: UDP port number of the secondary accounting server, which ranges from 1 to 65535 and defaults to 1813.

Description

Use the **secondary accounting** command to specify the secondary RADIUS accounting server.

Use the **undo secondary accounting** command to remove the configuration.

By default, no secondary RADIUS accounting server is specified.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The RADIUS service port configured on the device and that of the RADIUS server must be consistent.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **key**, **radius scheme**, **state**.

Examples

Specify the secondary accounting server for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary accounting 10.110.1.1 1813
```

secondary authentication (RADIUS scheme view)

Syntax

secondary authentication *ip-address* [*port-number*]

undo secondary authentication

View

RADIUS scheme view

Default Level

2: System level

Parameters

ip-address: IP address of the secondary authentication/authorization server, in dotted decimal notation. The default is 0.0.0.0.

port-number: UDP port number of the secondary authentication/authorization server, which ranges from 1 to 65535 and defaults to 1812.

Description

Use the **secondary authentication** command to specify the secondary RADIUS authentication/authorization server.

Use the **undo secondary authentication** command to remove the configuration.

By default, no secondary RADIUS authentication/authorization server is specified.

Note that:

- The IP addresses of the primary and secondary authentication/authorization servers cannot be the same. Otherwise, the configuration fails.
- The RADIUS service port configured on the device and that of the RADIUS server must be consistent.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **key**, **radius scheme**, **state**.

Examples

Specify the secondary authentication/authorization server for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary authentication 10.110.1.2 1812
```

security-policy-server

Syntax

security-policy-server *ip-address*

undo security-policy-server { *ip-address* | **all** }

View

RADIUS scheme view

Default Level

2: System level

Parameters

ip-address: IP address of a security policy server.

all: All IP addresses

Description

Use the **security-policy-server** command to specify a security policy server.

Use the **undo security-policy-server** command to remove one or all security policy servers.

By default, no security policy server is specified.

Note that:

- You can specify up to eight security policy servers for a RADIUS scheme.
- You can use the commands to change the settings only when no user is using the RADIUS scheme.

Related commands: **radius nas-ip**.

Examples

For RADIUS scheme **radius1**, set the IP address of a security policy server to 10.110.1.2.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] security-policy-server 10.110.1.2
```

server-type

Syntax

server-type { **extended** | **standard** }

undo server-type

View

RADIUS scheme view

Default Level

2: System level

Parameters

extended: Specifies the extended RADIUS server (generally iMC), which requires the RADIUS client and RADIUS server to interact according to the procedures and packet formats provisioned by the private RADIUS protocol.

standard: Specifies the standard RADIUS server, which requires the RADIUS client end and RADIUS server to interact according to the regulation and packet format of the standard RADIUS protocol (RFC 2865/2866 or newer).

Description

Use the **server-type** command to specify the RADIUS server type supported by the device.

Use the **undo server-type** command to restore the default.

By default, the supported RADIUS server type is **standard**.

Note that you can use the commands to change the setting only when no user is using the RADIUS scheme.

Related commands: **radius scheme**.

Examples

Set the RADIUS server type of RADIUS scheme **radius1** to **standard**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] server-type standard
```

state

Syntax

state { **primary** | **secondary** } { **accounting** | **authentication** } { **active** | **block** }

View

RADIUS scheme view

Default Level

2: System level

Parameters

primary: Sets the status of the primary RADIUS server.

secondary: Sets the status of the secondary RADIUS server.

accounting: Sets the status of the RADIUS accounting server.

authentication: Sets the status of the RADIUS authentication/authorization server.

active: Sets the status of the RADIUS server to **active**, namely the normal operation state.

block: Sets the status of the RADIUS server to **block**.

Description

Use the **state** command to set the status of a RADIUS server.

By default, every RADIUS server configured with an IP address in the RADIUS scheme is in the state of active.

Note that:

- When a primary server, authentication/authorization server or accounting server, fails, the device automatically turns to the secondary server.
- Once the primary server fails, the primary server turns into the blocked state, and the device turns to the secondary server. In this case, if the secondary server is available, the device triggers the primary server quiet timer. After the quiet timer times out, the status of the primary server is active again and the status of the secondary server remains the same. If the secondary server fails, the device restores the status of the primary server to active immediately. If the primary server has resumed, the device turns to use the primary server and stops communicating with the secondary server. After accounting starts, the communication between the client and the secondary server remains unchanged.
- When both the primary server and the secondary server are in the state of blocked, you need to set the status of the secondary server to active to use the secondary server for authentication. Otherwise, the switchover will not occur.
- If one server is in the active state while the other is blocked, the switchover will not take place even if the active server is not reachable.
- You can use this command to change the settings only when no user is using the RADIUS scheme.

Related commands: **radius scheme**, **primary authentication**, **secondary authentication**, **primary accounting**, **secondary accounting**.

Examples

Set the status of the secondary server in RADIUS scheme radius1 to **active**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state secondary authentication active
```

stop-accounting-buffer enable (RADIUS scheme view)

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

View

RADIUS scheme view

Default Level

2: System level

Parameters

None

Description

Use the **stop-accounting-buffer enable** command to enable the device to buffer stop-accounting requests getting no responses.

Use the **undo stop-accounting-buffer enable** command to disable the device from buffering stop-accounting requests getting no responses.

By default, the device is enabled to buffer stop-accounting requests getting no responses.

Since stop-accounting requests affect the charge to users, a NAS must make its best effort to send every stop-accounting request to the RADIUS accounting servers. For each stop-accounting request getting no response in the specified period of time, the NAS buffers and resends the packet until it receives a response or the number of transmission retries reaches the configured limit. In the latter case, the NAS discards the packet.

Note that you can use the commands to change the setting only when no user is using the RADIUS scheme.

Related commands: **reset stop-accounting-buffer**, **radius scheme**, **display stop-accounting-buffer**.

Examples

In RADIUS scheme **radius1**, enable the device to buffer the stop-accounting requests getting no responses.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-buffer enable
```

timer quiet (RADIUS scheme view)

Syntax

timer quiet *minutes*

undo timer quiet

View

RADIUS scheme view

Default Level

2: System level

Parameters

minutes: Primary server quiet period, in minutes. It ranges from 1 to 255 and defaults to 5.

Description

Use the **timer quiet** command to set the quiet timer for the primary server, that is, the duration that the status of the primary server stays blocked before resuming the active state.

Use the **undo timer quiet** command to restore the default.

Related commands: **display radius scheme**.

Examples

Set the quiet timer for the primary server to 10 minutes.

```
<Sysname> system-view
[Sysname] radius scheme test1
[Sysname-radius-test1] timer quiet 10
```

timer realtime-accounting (RADIUS scheme view)

Syntax

timer realtime-accounting *minutes*

undo timer realtime-accounting

View

RADIUS scheme view

Default Level

2: System level

Parameters

minutes: Real-time accounting interval in minutes, must be a multiple of 3 and in the range 3 to 60, with the default value being 12.

Description

Use the **timer realtime-accounting** command to set the real-time accounting interval.

Use the **undo timer realtime-accounting** command to restore the default.

Note that:

- For real-time accounting, a NAS must transmit the accounting information of online users to the RADIUS accounting server periodically. This command is for setting the interval.
- The setting of the real-time accounting interval somewhat depends on the performance of the NAS and the RADIUS server: a shorter interval requires higher performance. You are therefore recommended to adopt a longer interval when there are a large number of users (more than 1000, inclusive). The following table lists the recommended ratios of the interval to the number of users.

Table 2-3 Recommended ratios of the accounting interval to the number of users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
1000 or more	15 or more

Related commands: **retry realtime-accounting**, **radius scheme**.

Examples

Set the real-time accounting interval to 51 minutes for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer realtime-accounting 51
```

timer response-timeout (RADIUS scheme view)

Syntax

timer response-timeout *seconds*

undo timer response-timeout

View

RADIUS scheme view

Default Level

2: System level

Parameters

seconds: RADIUS server response timeout period in seconds. It ranges from 1 to 10 and defaults to 3.

Description

Use the **timer response-timeout** command to set the RADIUS server response timeout timer.

Use the **undo timer** command to restore the default.

Note that:

- If a NAS receives no response from the RADIUS server in a period of time after sending a RADIUS request (authentication/authorization or accounting request), it has to resend the request

so that the user has more opportunity to obtain the RADIUS service. The NAS uses the RADIUS server response timeout timer to control the transmission interval.

- A proper value for the RADIUS server response timeout timer can help improve the system performance. Set the timer based on the network conditions.
- The maximum total number of all types of retransmission attempts multiplied by the RADIUS server response timeout period cannot be greater than 75.

Related commands: **radius scheme**, **retry**.

Examples

Set the RADIUS server response timeout timer to 5 seconds for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer response-timeout 5
```

user-name-format (RADIUS scheme view)

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

View

RADIUS scheme view

Default Level

2: System level

Parameters

keep-original: Sends the username to the RADIUS server as it is input.

with-domain: Includes the ISP domain name in the username sent to the RADIUS server.

without-domain: Excludes the ISP domain name from the username sent to the RADIUS server.

Description

Use the **user-name-format** command to specify the format of the username to be sent to a RADIUS server.

By default, the ISP domain name is included in the username.

Note that:

- A username is generally in the format of userid@isp-name, of which isp-name is used by the device to determine the ISP domain to which a user belongs. Some earlier RADIUS servers, however, cannot recognize a username including an ISP domain name. Before sending a username including a domain name to such a RADIUS server, the device must remove the domain name. This command is thus provided for you to decide whether to include a domain name in a username to be sent to a RADIUS server.
- If a RADIUS scheme defines that the username is sent without the ISP domain name, do not apply the RADIUS scheme to more than one ISP domain, thus avoiding the confused situation where the RADIUS server regards two users in different ISP domains but with the same user ID as one.

- When 802.1X users use EAP authentication, the **user-name-format** command configured for a RADIUS scheme does not take effect and the device does not change the usernames from clients when forwarding them to the RADIUS server.
- If the RADIUS scheme is for wireless users, specify the **keep-original** keyword. Otherwise, authentication of the wireless users may fail.

Related commands: **radius scheme**.

Examples

Specify the device to remove the domain name in the username sent to the RADIUS servers for the RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] user-name-format without-domain
```

3 HWTACACS Configuration Commands

HWTACACS Configuration Commands

data-flow-format (HWTACACS scheme view)

Syntax

data-flow-format { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } } *

undo data-flow-format { **data** | **packet** }

View

HWTACACS scheme view

Default Level

2: System level

Parameters

data: Specifies the unit for data flows, which can be byte, kilobyte, megabyte, or gigabyte.

packet: Specifies the unit for data packets, which can be one-packet, kilo-packet, mega-packet, or giga-packet.

Description

Use the **data-flow-format** command to specify the unit for data flows or packets to be sent to a HWTACACS server.

Use the **undo data-flow-format** command to restore the default.

By default, the unit for data flows is **byte** and that for data packets is **one-packet**.

Related commands: **display hwtacacs**.

Examples

Define HWTACACS scheme **hwt1** to send data flows and packets destined for the TACACS server in kilobytes and kilo-packets.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] data-flow-format data kilo-byte packet kilo-packet
```

display hwtacacs

Syntax

display hwtacacs [*hwtacacs-scheme-name* [**statistics**]] [**slot** *slot-number*]

View

Any view

Default Level

2: System level

Parameters

hwtacacs-scheme-name: HWTACACS scheme name.

statistics: Displays complete statistics about the HWTACACS server.

slot *slot-number*: Specifies the specified member device in an IRF. The *slot-number* argument indicates the member device ID.

Description

Use the **display hwtacacs** command to display configuration information or statistics of the specified or all HWTACACS schemes.

Note that:

- If no HWTACACS scheme is specified, the command will display the configuration information of all HWTACACS schemes.
- If no slot number is specified, the command will display the configuration information of the HWTACACS scheme on the main processing unit.

Related commands: **hwtacacs scheme**.

Examples

Display configuration information about HWTACACS scheme **gy**.

```
<Sysname> display hwtacacs gy
  ------------------------------------------------------------------------
HWTACACS-server template name      : gy
  Primary-authentication-server    : 172.31.1.11:49
  Primary-authorization-server     : 172.31.1.11:49
  Primary-accounting-server       : 172.31.1.11:49
  Secondary-authentication-server   : 0.0.0.0:0
  Secondary-authorization-server    : 0.0.0.0:0
  Secondary-accounting-server      : 0.0.0.0:0
  Current-authentication-server    : 172.31.1.11:49
  Current-authorization-server     : 172.31.1.11:49
  Current-accounting-server       : 172.31.1.11:49
  NAS-IP-address                 : 0.0.0.0
  key authentication              : 790131
  key authorization               : 790131
  key accounting                 : 790131
  Quiet-interval(min)             : 5
  Realtime-accounting-interval(min) : 12
  Response-timeout-interval(sec)    : 5
  Acct-stop-PKT retransmit times    : 100
  Username format                : with-domain
  Data traffic-unit               : B
```

```
Packet traffic-unit            : one-packet
-----------------------------------------------------------------
```

Table 3-1 display hwtacacs command output description

Field	Description
HWTACACS-server template name	Name of the HWTACACS scheme
Primary-authentication-server	IP address and port number of the primary authentication server. If there is no primary authentication server specified, the value of this field is 0.0.0.0:0. This rule is also applicable to the following eight fields.
Primary-authorization-server	IP address and port number of the primary authorization server
Primary-accounting-server	IP address and port number of the primary accounting server
Secondary-authentication-server	IP address and port number of the secondary authentication server
Secondary-authorization-server	IP address and port number of the secondary authorization server
Secondary-accounting-server	IP address and port number of the secondary accounting server
Current-authentication-server	IP address and port number of the currently used authentication server
Current-authorization-server	IP address and port number of the currently used authorization server
Current-accounting-server	IP address and port number of the currently used accounting server
NAS-IP-address	IP address of the NAS If no NAS is specified, the value of this field is 0.0.0.0.
key authentication	Key for authentication
key authorization	Key for authorization
key accounting	Key for accounting
Quiet-interval	Quiet interval for the primary server
Realtime-accounting-interval	Real-time accounting interval
Response-timeout-interval	Server response timeout period
Acct-stop-PKT retransmit times	Number of stop-accounting packet transmission retries
Username format	with-domain Whether a user name includes the domain name
Data traffic-unit	Unit for data flows
Packet traffic-unit	Unit for data packets

display stop-accounting-buffer

Syntax

display stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name* [**slot** *slot-number*]

View

Any view

Default Level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies a HWTACACS scheme by its name, a string of 1 to 32 characters.

slot *slot-number*: Specifies the specified member device in an IRF. The *slot-number* argument indicates the member device ID.

Description

Use the **display stop-accounting-buffer** command to display information about the stop-accounting requests buffered in the device.

Related commands: **reset stop-accounting-buffer**, **stop-accounting-buffer enable**, **retry stop-accounting**.

Examples

Display information about the buffered stop-accounting requests for HWTACACS scheme **hwt1**.

```
<Sysname> display stop-accounting-buffer hwtacacs-scheme hwt1
Total 0 record(s) Matched
```

hwtacacs nas-ip

Syntax

hwtacacs nas-ip *ip-address*

undo hwtacacs nas-ip

View

System view

Default Level

2: System level

Parameters

ip-address: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

Description

Use the **hwtacacs nas-ip** command to set the IP address for the device to use as the source address of the HWTACACS packets to be sent to the server.

Use the **undo hwtacacs nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the HWTACACS packets to be sent to the server can avoid the situation where the packets sent back by the HWTACACS server cannot reach the device as the result of a physical interface failure.
- If you configure the command for more than one time, the last configuration takes effect.
- The **nas-ip** command in HWTACACS scheme view is only for the current HWTACACS scheme, while the **hwtacacs nas-ip** command in system view is for all HWTACACS schemes. However, the **nas-ip** command in HWTACACS scheme view overwrites the configuration of the **hwtacacs nas-ip** command.

Related commands: **nas-ip**.

Examples

Set the IP address for the device to use as the source address of the HWTACACS packets to **129.10.10.1**.

```
<Sysname> system-view
[Sysname] hwtacacs nas-ip 129.10.10.1
```

hwtacacs scheme

Syntax

hwtacacs scheme *hwtacacs-scheme-name*

undo hwtacacs scheme *hwtacacs-scheme-name*

View

System view

Default Level

3: Manage level

Parameters

hwtacacs-scheme-name: HWTACACS scheme name, a case-insensitive string of 1 to 32 characters.

Description

Use the **hwtacacs scheme** command to create an HWTACACS scheme and enter HWTACACS scheme view.

Use the **undo hwtacacs scheme** command to delete an HWTACACS scheme.

By default, no HWTACACS scheme exists.

Note that you cannot delete an HWTACACS scheme with online users.

Examples

Create an HWTACACS scheme named **hwt1** and enter HWTACACS scheme view.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1]
```

key (HWTACACS scheme view)

Syntax

key { **accounting** | **authentication** | **authorization** } *string*

undo key { **accounting** | **authentication** | **authorization** } *string*

View

HWTACACS scheme view

Default Level

2: System level

Parameters

accounting: Sets the shared key for HWTACACS accounting packets.

authentication: Sets the shared key for HWTACACS authentication packets.

authorization: Sets the shared key for HWTACACS authorization packets.

string: Shared key, a string of 1 to 16 characters.

Description

Use the **key** command to set the shared key for HWTACACS authentication, authorization, or accounting packets.

Use the **undo key** command to remove the configuration.

By default, no shared key is configured.

Related commands: **display hwtacacs**.

Examples

Set the shared key for HWTACACS accounting packets to **hello** for HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key accounting hello
```

nas-ip (HWTACACS scheme view)

Syntax

nas-ip *ip-address*

undo nas-ip

View

HWTACACS scheme view

Default Level

2: System level

Parameters

ip-address: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

Description

Use the **nas-ip** command to set the IP address for the device to use as the source address of the HWTACACS packets to be sent to the server.

Use the **undo nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the HWTACACS packets to be sent to the server can avoid the situation where the packets sent back by the HWTACACS server cannot reach the device as the result of a physical interface failure.
- If you configure the command for more than one time, the last configuration takes effect.
- The **nas-ip** command in HWTACACS scheme view is only for the current HWTACACS scheme, while the **hwtacacs nas-ip** command in system view is for all HWTACACS schemes. However, the **nas-ip** command in HWTACACS scheme view overwrites the configuration of the **hwtacacs nas-ip** command.

Related commands: **hwtacacs nas-ip**.

Examples

Set the IP address for the device to use as the source address of the HWTACACS packets to 10.1.1.1.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] nas-ip 10.1.1.1
```

primary accounting (HWTACACS scheme view)

Syntax

primary accounting *ip-address* [*port-number*]

undo primary accounting

View

HWTACACS scheme view

Default Level

2: System level

Parameters

ip-address: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description

Use the **primary accounting** command to specify the primary HWTACACS accounting server.

Use the **undo primary accounting** command to remove the configuration.

By default, no primary HWTACACS accounting server is specified.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an accounting server only when no active TCP connection for sending accounting packets is using it.

Examples

Specify the primary accounting server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme test1
[Sysname-hwtacacs-test1] primary accounting 10.163.155.12 49
```

primary authentication (HWTACACS scheme view)

Syntax

primary authentication *ip-address* [*port-number*]

undo primary authentication

View

HWTACACS scheme view

Default Level

2: System level

Parameters

ip-address: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description

Use the **primary authentication** command to specify the primary HWTACACS authentication server.

Use the **undo primary authentication** command to remove the configuration.

By default, no primary HWTACACS authentication server is specified.

Note that:

- The IP addresses of the primary and secondary authentication servers cannot be the same. Otherwise, the configuration fails.

- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authentication server only when no active TCP connection for sending authentication packets is using it.

Related commands: **display hwtacacs**.

Examples

Specify the primary authentication server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authentication 10.163.155.13 49
```

primary authorization

Syntax

primary authorization *ip-address* [*port-number*]

undo primary authorization

View

HWTACACS scheme view

Default Level

2: System level

Parameters

ip-address: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description

Use the **primary authorization** command to specify the primary HWTACACS authorization server.

Use the **undo primary authorization** command to remove the configuration.

By default, no primary HWTACACS authorization server is specified.

Note that:

- The IP addresses of the primary and secondary authorization servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authorization server only when no active TCP connection for sending authorization packets is using it.

Related commands: **display hwtacacs**.

Examples

Configure the primary authorization server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authorization 10.163.155.13 49
```

reset hwtacacs statistics

Syntax

reset hwtacacs statistics { **accounting** | **all** | **authentication** | **authorization** } [**slot** *slot-number*]

View

User view

Default Level

1: Monitor level

Parameters

accounting: Clears HWTACACS accounting statistics.

all: Clears all HWTACACS statistics.

authentication: Clears HWTACACS authentication statistics.

authorization: Clears HWTACACS authorization statistics.

slot *slot-number*: Clears HWTACACS statistics on the specified member device in an IRF. The *slot-number* argument indicates the member device ID.

Description

Use the **reset hwtacacs statistics** command to clear HWTACACS statistics.

Related commands: **display hwtacacs**.

Examples

Clear all HWTACACS statistics.

```
<Sysname> reset hwtacacs statistics all
```

reset stop-accounting-buffer

Syntax

reset stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name* [**slot** *slot-number*]

View

User view

Default Level

2: System level

Parameters

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies a HWTACACS scheme by its name, a string of 1 to 32 characters.

slot *slot-number*: Specifies the specified member device in an IRF. The *slot-number* argument indicates the member device ID.

Description

Use the **reset stop-accounting-buffer** command to clear the buffered stop-accounting requests that get no responses.

Related commands: **stop-accounting-buffer enable**, **retry stop-accounting**, **display stop-accounting-buffer**.

Examples

Clear the buffered stop-accounting requests for HWTACACS scheme **hwt1**.

```
<Sysname> reset stop-accounting-buffer hwtacacs-scheme hwt1
```

retry stop-accounting (HWTACACS scheme view)

Syntax

retry stop-accounting *retry-times*

undo retry stop-accounting

View

HWTACACS scheme view

Default Level

2: System level

Parameters

retry-times: Maximum number of stop-accounting request transmission attempts. It ranges from 1 to 300 and defaults to 100.

Description

Use the **retry stop-accounting** command to set the maximum number of stop-accounting request transmission attempts.

Use the **undo retry stop-accounting** command to restore the default.

Related commands: **reset stop-accounting-buffer**, **hwtacacs scheme**, **display stop-accounting-buffer**.

Examples

Set the maximum number of stop-accounting request transmission attempts to 50.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] retry stop-accounting 50
```

secondary accounting (HWTACACS scheme view)

Syntax

secondary accounting *ip-address* [*port-number*]

undo secondary accounting

View

HWTACACS scheme view

Default Level

2: System level

Parameters

ip-address: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description

Use the **secondary accounting** command to specify the secondary HWTACACS accounting server.

Use the **undo secondary accounting** command to remove the configuration.

By default, no secondary HWTACACS accounting server is specified.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an accounting server only when no active TCP connection for sending accounting packets is using it.

Examples

Specify the secondary accounting server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary accounting 10.163.155.12 49
```

secondary authentication (HWTACACS scheme view)

Syntax

secondary authentication *ip-address* [*port-number*]

undo secondary authentication

View

HWTACACS scheme view

Default Level

2: System level

Parameters

ip-address: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description

Use the **secondary authentication** command to specify the secondary HWTACACS authentication server.

Use the **undo secondary authentication** command to remove the configuration.

By default, no secondary HWTACACS authentication server is specified.

Note that:

- The IP addresses of the primary and secondary authentication servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authentication server only when no active TCP connection for sending authentication packets is using it.

Related commands: **display hwtacacs**.

Examples

Specify the secondary authentication server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authentication 10.163.155.13 49
```

secondary authorization

Syntax

secondary authorization *ip-address* [*port-number*]

undo secondary authorization

View

HWTACACS scheme view

Default Level

2: System level

Parameters

ip-address: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description

Use the **secondary authorization** command to specify the secondary HWTACACS authorization server.

Use the **undo secondary authorization** command to remove the configuration.

By default, no secondary HWTACACS authorization server is specified.

Note that:

- The IP addresses of the primary and secondary authorization servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authorization server only when no active TCP connection for sending authorization packets is using it.

Related commands: **display hwtacacs**.

Examples

Configure the secondary authorization server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authorization 10.163.155.13 49
```

stop-accounting-buffer enable (HWTACACS scheme view)

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

View

HWTACACS scheme view

Default Level

2: System level

Parameters

None

Description

Use the **stop-accounting-buffer enable** command to enable the device to buffer stop-accounting requests getting no responses.

Use the **undo stop-accounting-buffer enable** command to disable the device from buffering stop-accounting requests getting no responses.

By default, the device is enabled to buffer stop-accounting requests getting no responses.

Since stop-accounting requests affect the charge to users, a NAS must make its best effort to send every stop-accounting request to the HWTACACS accounting servers. For each stop-accounting request getting no response in the specified period of time, the NAS buffers and resends the packet

until it receives a response or the number of transmission retries reaches the configured limit. In the latter case, the NAS discards the packet.

Related commands: **reset stop-accounting-buffer**, **hwtacacs scheme**, **display stop-accounting-buffer**.

Examples

In HWTACACS scheme **hwt1**, enable the device to buffer the stop-accounting requests getting no responses.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] stop-accounting-buffer enable
```

timer quiet (HWTACACS scheme view)

Syntax

timer quiet *minutes*

undo timer quiet

View

HWTACACS scheme view

Default Level

2: System level

Parameters

minutes: Primary server quiet period, in minutes. It ranges from 1 to 255 and defaults to 5.

Description

Use the **timer quiet** command to set the quiet timer for the primary server, that is, the duration that the status of the primary server stays blocked before resuming the active state.

Use the **undo timer quiet** command to restore the default.

Related commands: **display hwtacacs**.

Examples

Set the quiet timer for the primary server to 10 minutes.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer quiet 10
```

timer realtime-accounting (HWTACACS scheme view)

Syntax

timer realtime-accounting *minutes*

undo timer realtime-accounting

View

HWTACACS scheme view

Default Level

2: System level

Parameters

minutes: Real-time accounting interval in minutes. It is a multiple of 3 in the range 3 to 60 and defaults to 12.

Description

Use the **timer realtime-accounting** command to set the real-time accounting interval.

Use the **undo timer realtime-accounting** command to restore the default.

Note that:

- For real-time accounting, a NAS must transmit the accounting information of online users to the HWTACACS accounting server periodically. This command is for setting the interval.
- The setting of the real-time accounting interval somewhat depends on the performance of the NAS and the HWTACACS server: a shorter interval requires higher performance. You are therefore recommended to adopt a longer interval when there are a large number of users (more than 1000, inclusive). The following table lists the recommended ratios of the interval to the number of users.

Table 3-2 Recommended ratios of the accounting interval to the number of users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
1000 or more	15 or more

Examples

Set the real-time accounting interval to 51 minutes for HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer realtime-accounting 51
```

timer response-timeout (HWTACACS scheme view)

Syntax

timer response-timeout *seconds*

undo timer response-timeout

View

HWTACACS scheme view

Default Level

2: System level

Parameters

seconds: HWTACACS server response timeout period in seconds. It ranges from 1 to 300 and defaults to 5.

Description

Use the **timer response-timeout** command to set the HWTACACS server response timeout timer.

Use the **undo timer** command to restore the default.

As HWTACACS is based on TCP, the timeout of the server response timeout timer and/or the TCP timeout timer will cause the device to be disconnected from the HWTACACS server.

Related commands: **display hwtacacs**.

Examples

Set the HWTACACS server response timeout timer to 30 seconds for HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer response-timeout 30
```

user-name-format (HWTACACS scheme view)

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

View

HWTACACS scheme view

Default Level

2: System level

Parameters

keep-original: Sends the username to the HWTACACS server as it is input.

with-domain: Includes the ISP domain name in the username sent to the HWTACACS server.

without-domain: Excludes the ISP domain name from the username sent to the HWTACACS server.

Description

Use the **user-name-format** command to specify the format of the username to be sent to a HWTACACS server.

By default, the ISP domain name is included in the username.

Note that:

- A username is generally in the format of userid@isp-name, of which isp-name is used by the device to determine the ISP domain to which a user belongs. Some earlier HWTACACS servers, however, cannot recognize a username including an ISP domain name. Before sending a username including a domain name to such a HWTACACS server, the device must remove the

domain name. This command is thus provided for you to decide whether to include a domain name in a username to be sent to a HWTACACS server.

- If a HWTACACS scheme defines that the username is sent without the ISP domain name, do not apply the HWTACACS scheme to more than one ISP domain, thus avoiding the confused situation where the HWTACACS server regards two users in different ISP domains but with the same userid as one.
- If the HWTACACS scheme is for wireless users, specify the **keep-original** keyword. Otherwise, authentication of the wireless users may fail.

Related commands: **hwtacacs scheme**.

Examples

Specify the device to remove the ISP domain name in the username sent to the HWTACACS servers for the HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] user-name-format without-domain
```

4 802.1X Configuration Commands

802.1X Configuration Commands

display dot1x

Syntax

display dot1x [**sessions** | **statistics**] [**interface** *interface-list*]

View

Any view

Default Level

1: Monitor level

Parameters

sessions: Displays 802.1X session information.

statistics: Displays 802.1X statistics.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use the **display dot1x** command to display information about 802.1X.

If you specify neither the **sessions** keyword nor the **statistics** keyword, the command displays all information about 802.1X, including session information, statistics, and configurations.

Related commands: reset dot1x statistics, dot1x, dot1x retry, dot1x max-user, dot1x port-control, dot1x port-method, dot1x timer.

Examples

Display all information about 802.1X.

```
<Sysname> display dot1x
Equipment 802.1X protocol is enabled
CHAP authentication is enabled
EAD quick deploy is enabled

Configuration: Transmit Period    30 s,  Handshake Period      15 s
               Quiet Period       60 s,  Quiet Period Timer is disabled
               Supp Timeout       30 s,  Server Timeout        100 s
```

```
            Reauth Period    3600 s
            The maximal retransmitting times        3
EAD quick deploy configuration:
            URL: http://192.168.19.23
            Free IP: 192.168.19.0 255.255.255.0
            EAD timeout:   30m

The maximum 802.1X user resource number is 1024 per slot
Total current used 802.1X resource number is 1

GigabitEthernet1/0/1  is link-up
  802.1X protocol is enabled
   Handshake is disabled
  Handshake secure is disabled
  Periodic reauthentication is disabled
  The port is an authenticator
  Authenticate Mode is Auto
  802.1X Multicast-trigger is enabled
  Mandatory authentication domain: NOT configured
  Port Control Type is Mac-based
  Guest VLAN: 4
  Max number of on-line users is 256

  EAPOL Packet: Tx 1087, Rx 986
  Sent EAP Request/Identity Packets : 943
      EAP Request/Challenge Packets: 60
      EAP Success Packets: 29, Fail Packets: 55
  Received EAPOL Start Packets : 60
          EAPOL LogOff Packets: 24
          EAP Response/Identity Packets : 724
          EAP Response/Challenge Packets: 54
          Error Packets: 0
1. Authenticated user : MAC address: 0015-e9a6-7cfe

  Controlled User(s) amount to 1
```

Table 4-1 display dot1x command output description

Field	Description
Equipment 802.1X protocol is enabled	Indicates whether 802.1X is enabled globally
CHAP authentication is enabled	Indicates whether CHAP authentication is enabled
EAD quick deploy is enabled	Indicates whether EAD quick deployment is enabled
Transmit Period	Setting of the username request timeout timer
Handshake Period	Setting of the handshake timer
Reauth Period	Setting of the periodic re-authentication timer

Field	Description
Quiet Period	Setting of the quiet timer
Quiet Period Timer is disabled	Indicates whether the quiet timer is enabled
Supp Timeout	Setting of the supplicant timeout timer
Server Timeout	Setting of the server timeout timer
The maximal retransmitting times	Maximum number of attempts for the authenticator to send authentication requests to the supplicant
EAD quick deploy configuration	EAD quick deployment configurations
URL	Redirect URL for IE users
Free IP	Accessible network segment
EAD timeout	EAD rule timeout time
The maximum 802.1X user resource number per slot	Maximum number of supplicants supported per board
Total current used 802.1X resource number	Total number of online users
GigabitEthernet1/0/1 is link-up	Status of port GigabitEthernet 1/0/1
802.1X protocol is disabled	Indicates whether 802.1X is enabled on the port
Handshake is disabled	Indicates whether handshake is enabled on the port
Handshake secure is disabled	Indicates whether handshake secure is enabled on the port
Periodic reauthentication is disabled	Indicates whether periodic re-authentication is enabled on the port
The port is an authenticator	Role of the port
Authenticate Mode is Auto	Access control mode for the port
802.1X Multicast-trigger is enabled	Indicates whether the 802.1X multicast-trigger function is enabled
Mandatory authentication domain	Mandatory authentication domain for users accessing the port
Port Control Type is Mac-based	Access control method for the port
Guest VLAN	Guest VLAN configured for the port. “NOT configured” means that no guest VLAN is configured.
Max number of on-line users	Maximum number of users supported on the port
EAPOL Packet	Counts of EAPOL packets sent (Tx) and received (Rx)
Sent EAP Request/Identity Packets	Number of EAP Request/Identity packets sent
EAP Request/Challenge Packets	Number of EAP Request/Challenge packets sent
EAP Success Packets	Number of EAP Success packets sent
Received EAPOL Start Packets	Number of EAPOL Start packets received
EAPOL LogOff Packets	Number of EAPOL LogOff packets received

Field	Description
EAP Response/Identity Packets	Number of EAP Response/Identity packets received
EAP Response/Challenge Packets	Number of EAP Response/Challenge packets received
Error Packets	Number of erroneous packets received
Authenticated user	User that has passed the authentication
Controlled User(s) amount	Number of controlled users on the port

dot1x

Syntax

In system view:

dot1x [**interface** *interface-list*]

undo dot1x [**interface** *interface-list*]

In Ethernet interface view:

dot1x

undo dot1x

View

System view, interface view

Default Level

2: System level

Parameters

interface *interface-list*: Specifies a port list, which can contain multiple ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use the **dot1x** command in system view to enable 802.1X globally.

Use the **undo dot1x** command in system view to disable 802.1X globally.

Use the **dot1x interface** *interface-list* command in system view or the **dot1x** command in interface view to enable 802.1X for specified ports.

Use the **undo dot1x interface** *interface-list* command in system view or the **undo dot1x** command in interface view to disable 802.1X for specified ports.

By default, 802.1X is neither enabled globally nor enabled for any port.

Note that:

- 802.1X must be enabled both globally in system view and for the intended ports in system view or interface view. Otherwise, it does not function.
- You can configure 802.1X parameters either before or after enabling 802.1X.

Related commands: **display dot1x**.

Examples

Enable 802.1X for ports GigabitEthernet 1/0/1, and GigabitEthernet 1/0/5 to GigabitEthernet 1/0/7.

```
<Sysname> system-view
[Sysname] dot1x interface GigabitEthernet 1/0/1 GigabitEthernet 1/0/5 to GigabitEthernet
1/0/7
```

Or

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface GigabitEthernet 1/0/5
[Sysname-GigabitEthernet1/0/5] dot1x
[Sysname-GigabitEthernet1/0/5] quit
[Sysname] interface GigabitEthernet 1/0/6
[Sysname-GigabitEthernet1/0/6] dot1x
[Sysname-GigabitEthernet1/0/6] quit
[Sysname] interface GigabitEthernet 1/0/7
[Sysname-GigabitEthernet1/0/7] dot1x
```

Enable 802.1X globally.

```
<Sysname> system-view
[Sysname] dot1x
```

dot1x authentication-method

Syntax

dot1x authentication-method { **chap** | **eap** | **pap** }

undo dot1x authentication-method

View

System view

Default Level

2: System level

Parameters

chap: Authenticates supplicants using CHAP.

eap: Authenticates supplicants using EAP.

pap: Authenticates supplicants using PAP.

Description

Use the **dot1x authentication-method** command to set the 802.1X authentication method.

Use the **undo dot1x authentication-method** command to restore the default.

By default, CHAP is used.

- The password authentication protocol (PAP) transports passwords in clear text.
- The challenge handshake authentication protocol (CHAP) transports only usernames over the network. Compared with PAP, CHAP provides better security.
- With EAP relay authentication, the authenticator encapsulates 802.1X user information in the EAP attributes of RADIUS packets and sends the packets to the RADIUS server for authentication; it does not need to repackage the EAP packets into standard RADIUS packets for authentication. In this case, you can configure the **user-name-format** command but it does not take effect. For information about the **user-name-format** command, refer to *AAA Commands* in the *Security Volume*.

Note that:

- Local authentication supports PAP and CHAP.
- For RADIUS authentication, the RADIUS server must be configured accordingly to support PAP, CHAP, or EAP authentication.

Related commands: **display dot1x**.

Examples

Set the 802.1X authentication method to PAP.

```
<Sysname> system-view
[Sysname] dot1x authentication-method pap
```

dot1x guest-vlan

Syntax

In system view:

dot1x guest-vlan *guest-vlan-id* [**interface** *interface-list*]

undo dot1x guest-vlan [**interface** *interface-list*]

In interface view:

dot1x guest-vlan *guest-vlan-id*

undo dot1x guest-vlan

View

System view, Layer 2 Ethernet interface view

Default Level

2: System level

Parameters

guest-vlan-id: ID of the VLAN to be specified as the guest VLAN, in the range 1 to 4094. It must already exist.

interface *interface-list*: Specifies a port list. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use the **dot1x guest-vlan** command to configure the guest VLAN for specified or all ports.

Use the **undo dot1x guest-vlan** command to remove the guest VLAN(s) configured for specified or all ports.

By default, a port is configured with no guest VLAN.

Currently, on the S4210G series Ethernet switches, a guest VLAN can be only a port-based guest VLAN (PGV), which is supported on a port that uses the access control method of **portbased**.

Note that:

- In system view, this command configures a guest VLAN for all Layer 2 Ethernet ports if you do not specify the *interface-list* argument, and configures a guest VLAN for specified ports if you specify the *interface-list* argument.
- In interface view, you cannot specify the *interface-list* argument and can only configure guest VLAN for the current port.
- You must enable 802.1X for a guest VLAN to take effect.
- You must enable the 802.1X multicast trigger function for a PGV to take effect.
- After an PGV takes effect, if you change the port access method from **portbased** to **macbased**, the port will leave the guest VLAN.
- You are not allowed to delete a VLAN that is configured as a guest VLAN. To delete such a VLAN, you need to remove the guest VLAN configuration first.
- You cannot configure both the guest VLAN function and the free IP function on a port.

Related commands: **dot1x**; **dot1x port-method**; **dot1x multicast-trigger**; **mac-vlan enable**, and **display mac-vlan** in *VLAN Commands* in the *Access Volume*.

Examples

Specify port GigabitEthernet 1/0/1 to use VLAN 999 as its guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 999 interface GigabitEthernet 1/0/1
```

Specify ports GigabitEthernet 1/0/2 to GigabitEthernet 1/0/5 to use VLAN 10 as its guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 10 interface GigabitEthernet 1/0/2 to GigabitEthernet 1/0/5
```

Specify all ports to use VLAN 7 as their guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 7
```

Specify port GigabitEthernet 1/0/7 to use VLAN 3 as its guest VLAN.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/7
[Sysname-GigabitEthernet1/0/7] dot1x guest-vlan 3
```

dot1x handshake

Syntax

dot1x handshake

undo dot1x handshake

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **dot1x handshake** command to enable the online user handshake function so that the device can periodically send handshake messages to the client to check whether a user is online.

Use the **undo dot1x handshake** command to disable the function.

By default, the function is enabled.

Note that: To ensure that the online user handshake function can work normally, you are recommended to use the iNode 802.1X client software.

Examples

Enable online user handshake.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/4
[Sysname-GigabitEthernet1/0/4] dot1x handshake
```

dot1x mandatory-domain

Syntax

dot1x mandatory-domain *domain-name*

undo dot1x mandatory-domain

View

Interface view

Default Level

2: System level

Parameters

domain-name: ISP domain name, a case-insensitive string of 1 to 24 characters.

Description

Use the **dot1x mandatory-domain** command to specify the mandatory authentication domain for users accessing the port.

Use the **undo dot1x mandatory-domain** command to remove the mandatory authentication domain.

By default, no mandatory authentication domain is specified.

Note that:

- When authenticating an 802.1X user trying to access the port, the system selects an authentication domain in the following order: the mandatory domain, the ISP domain specified in the username, and the default ISP domain.
- The specified mandatory authentication domain must exist.
- On a port configured with a mandatory authentication domain, the user domain name displayed by the **display connection** command is the name of the mandatory authentication domain. For detailed information about the **display connection** command, refer to *AAA Commands* in the *Security Volume*.

Related commands: **display dot1x**.

Examples

Configure the mandatory authentication domain **my-domain** for 802.1X users on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x mandatory-domain my-domain
```

After 802.1X user **usera** passes the authentication, display the user connection information on GigabitEthernet 1/0/1.

```
[Sysname-GigabitEthernet1/0/1] display connection interface GigabitEthernet 1/0/1

Index=68  ,Username=usera@my-domian
MAC=0015-e9a6-7cfe   ,IP=3.3.3.3
 Total 1 connection(s) matched.
```

dot1x max-user

Syntax

In system view:

dot1x max-user *user-number* [**interface** *interface-list*]

undo dot1x max-user [**interface** *interface-list*]

In Ethernet interface view:

dot1x max-user *user-number*

undo dot1x max-user

View

System view, Ethernet interface view

Default Level

2: System level

Parameters

user-number: Maximum number of users to be supported simultaneously. The valid settings and the default may vary by device.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use the **dot1x max-user** command to set the maximum number of users to be supported simultaneously for specified or all ports.

Use the **undo dot1x max-user** command to restore the default.

With no interface specified, the command sets the threshold for all ports.

Related commands: **display dot1x**.

Examples

Set the maximum number of users for port GigabitEthernet 1/0/1 to support simultaneously as 32.

```
<Sysname> system-view
[Sysname] dot1x max-user 32 interface GigabitEthernet 1/0/1
```

Or

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x max-user 32
```

dot1x multicast-trigger

Syntax

dot1x multicast-trigger

undo dot1x multicast-trigger

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **dot1x multicast-trigger** command to enable the multicast trigger function of 802.1X to send multicast trigger messages to the clients periodically.

Use the **undo dot1x multicast-trigger** command to disable this function.

By default, the multicast trigger function is enabled.

Related commands: **display dot1x**.

Examples

Disable the multicast trigger function for interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo dot1x multicast-trigger
```

dot1x port-control

Syntax

In system view:

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** } [**interface** *interface-list*]

undo dot1x port-control [**interface** *interface-list*]

In Ethernet interface view:

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** }

undo dot1x port-control

View

System view, Ethernet interface view

Default Level

2: System level

Parameters

authorized-force: Places the specified or all ports in the authorized state, allowing users of the ports to access the network without authentication.

auto: Places the specified or all ports in the unauthorized state initially to allow only EAPOL frames to pass, and turns the ports into the authorized state to allow access to the network after the users pass authentication. This is the most common choice.

unauthorized-force: Places the specified or all ports in the unauthorized state, denying any access requests from users of the ports.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use the **dot1x port-control** command to set the access control mode for specified or all ports.

Use the **undo dot1x port-control** command to restore the default.

The default access control mode is **auto**.

Related commands: **display dot1x**.

Examples

Set the access control mode of port GigabitEthernet 1/0/1 to **unauthorized-force**.

```
<Sysname> system-view
[Sysname] dot1x port-control unauthorized-force interface GigabitEthernet 1/0/1
```

Or

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x port-control unauthorized-force
```

dot1x port-method

Syntax

In system view:

dot1x port-method { **macbased** | **portbased** } [**interface** *interface-list*]

undo dot1x port-method [**interface** *interface-list*]

In Ethernet interface view:

dot1x port-method { **macbased** | **portbased** }

undo dot1x port-method

View

System view, Ethernet interface view

Default Level

2: System level

Parameters

macbased: Specifies to use the **macbased** authentication method. With this method, each user of a port must be authenticated separately, and when an authenticated user goes offline, no other users are affected.

portbased: Specifies to use the **portbased** authentication method. With this method, after the first user of a port passes authentication, all other users of the port can access the network without authentication, and when the first user goes offline, all other users get offline at the same time.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use the **dot1x port-method** command to set the access control method for specified or all ports.

Use the **undo dot1x port-method** command to restore the default.

The default access control method is **macbased**.

Related commands: **display dot1x**.

Examples

Set the access control method to **portbased** for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] dot1x port-method portbased interface GigabitEthernet 1/0/1
```

Or

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x port-method portbased
```

dot1x quiet-period

Syntax

dot1x quiet-period

undo dot1x quiet-period

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **dot1x quiet-period** command to enable the quiet timer function.

Use the **undo dot1x quiet-period** command to disable the function.

By default, the function is disabled.

After a supplicant fails the authentication, the authenticator refuses further authentication requests from the supplicant in the period dictated by the quiet timer.

Related commands: **display dot1x**, **dot1x timer**.

Examples

Enable the quiet timer.

```
<Sysname> system-view
[Sysname] dot1x quiet-period
```

dot1x re-authenticate

Syntax

dot1x re-authenticate

undo dot1x re-authenticate

View

Ethernet interface view

Default Level

2: System level

Parameters

None

Description

Use the **dot1x re-authenticate** command to enable the periodic re-authentication function.

Use the **undo dot1x re-authenticate** command to restore the default.

By default, this function is disabled.

After periodic re-authentication is enabled on a port, the device will perform 802.1X authentication for online users on the port at the interval specified by the periodic re-authentication timer (which is configured by the **dot1x timer reauth-period** command). This is intended to track the connection status of online users and update the authorization attributes assigned by the server, such as the ACL, VLAN, and QoS Profile, ensuring that the users are in normal online state.

Related commands: **dot1x timer reauth-period**.

Examples

Enable the 802.1X re-authentication function on GigabitEthernet1/0/1 and configure the periodic re-authentication interval as 1800 seconds.

```
<Sysname> system-view
[Sysname] dot1x timer reauth-period 1800
[Sysname] interface gigabitethernet 1/0/1
[Sysname-Gigabitethernet1/0/1] dot1x re-authenticate
```

dot1x retry

Syntax

dot1x retry *max-retry-value*

undo dot1x retry

View

System view

Default Level

2: System level

Parameters

max-retry-value: Maximum number of attempts to send an authentication request to a supplicant, in the range 1 to 10.

Description

Use the **dot1x retry** command to set the maximum number of attempts to send an authentication request to a supplicant.

Use the **undo dot1x retry** command to restore the default.

By default, the authenticator can send an authentication request to a supplicant twice at most.

Note that after sending an authentication request to a supplicant, the authenticator may retransmit the request if it does not receive any response at an interval specified by the username request timeout timer or supplicant timeout timer. The number of retransmission attempts is one less than the value set by this command.

Related commands: **display dot1x**.

Examples

Set the maximum number of attempts to send an authentication request to a supplicant as 9.

```
<Sysname> system-view
[Sysname] dot1x retry 9
```

dot1x timer

Syntax

dot1x timer { **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* }

undo dot1x timer { **handshake-period** | **quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period** }

View

System view

Default Level

2: System level

Parameters

handshake-period-value: Setting for the handshake timer in seconds. It ranges from 5 to 1024 and defaults to 15.

quiet-period-value: Setting for the quiet timer in seconds. It ranges from 10 to 120 and defaults to 60.

reauth-period-value: Setting for the periodic re-authentication timer in seconds. It ranges from 60 to 7200 and defaults to 3600.

server-timeout-value: Setting for the server timeout timer in seconds. It ranges from 100 to 300 and defaults to 100.

supp-timeout-value: Setting for the supplicant timeout timer in seconds. It ranges from 1 to 120 and defaults to 30.

tx-period-value: Setting for the username request timeout timer in seconds. It ranges from 10 to 120 and defaults to 30.

Description

Use the **dot1x timer** command to set 802.1X timers.

Use the **undo dot1x timer** command to restore the defaults.

Several timers are used in the 802.1X authentication process to guarantee that the supplicants, the authenticators, and the RADIUS server interact with each other in a reasonable manner. You can use this command to set these timers:

- Handshake timer (handshake-period): After a supplicant passes authentication, the authenticator sends to the supplicant handshake requests at this interval to check whether the supplicant is online. If the authenticator receives no response after sending the allowed maximum number of handshake requests, it considers that the supplicant is offline.
- Quiet timer (quiet-period): When a supplicant fails the authentication, the authenticator refuses further authentication requests from the supplicant in this period of time.
- Periodic re-authentication timer (reauth-period): If you enable periodic re-authentication on a port (by the **dot1x re-authenticate** command), the device will re-authenticate online users on the port at the interval specified by this timer. If you change the re-authentication interval when there are users online, the device will continue to re-authenticate such users according to the original re-authentication interval setting for one time. Then the device will use the new interval for re-authentication of all online users.
- Server timeout timer (server-timeout): Once an authenticator sends a RADIUS Access-Request packet to the authentication server, it starts this timer. If this timer expires but it receives no response from the server, it retransmits the request.
- Supplicant timeout timer (supp-timeout): Once an authenticator sends an EAP-Request/MD5 Challenge frame to a supplicant, it starts this timer. If this timer expires but it receives no response from the supplicant, it retransmits the request.
- Username request timeout timer (tx-period): Once an authenticator sends an EAP-Request/Identity frame to a supplicant, it starts this timer. If this timer expires but it receives no response from the supplicant, it retransmits the request. In addition, to be compatible with clients that do not send EAPOL-Start requests unsolicitedly, the device multicasts EAP-Request/Identity frame periodically to detect the clients, with the multicast interval defined by tx-period.

It is unnecessary to change the timers unless in some special or extreme network environments. The change of a timer takes effect immediately.

Related commands: **display dot1x**.

Examples

Set the server timeout timer to 150 seconds.

```
<Sysname> system-view
[Sysname] dot1x timer server-timeout 150
```

reset dot1x statistics

Syntax

reset dot1x statistics [**interface** *interface-list*]

View

User view

Default Level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

Description

Use the **reset dot1x statistics** command to clear 802.1X statistics.

With the **interface** *interface-list* argument specified, the command clears 802.1X statistics on the specified ports. With the argument unspecified, the command clears global 802.1X statistics and 802.1X statistics on all ports.

Related commands: **display dot1x**.

Examples

Clear 802.1X statistics on port GigabitEthernet 1/0/1.

```
<Sysname> reset dot1x statistics interface GigabitEthernet 1/0/1
```

5 EAD Fast Deployment Configuration Commands

EAD Fast Deployment Configuration Commands

dot1x free-ip

Syntax

dot1x free-ip *ip-address* { *mask-address* | *mask-length* }

undo dot1x free-ip { *ip-address* { *mask* | *mask-length* } | **all** }

View

System view

Default Level

2: System level

Parameters

ip-address: IP address of the freely accessible network segment, also called a free IP.

mask: Mask of the freely accessible network segment.

mask-length: Length of the mask of the freely accessible network segment.

all: Specifies all the freely accessible network segments.

Description

Use the **dot1x free-ip** command to configure a freely accessible network segment, that is, a network segment that users can access before passing 802.1X authentication.

Use the **undo dot1x free-ip** command to remove one or all freely accessible network segments.

By default, no freely accessible network segment is configured.

Note that:

- The free IP function is mutually exclusive with the global MAC authentication function, the port security function, and the guest VLAN function on a port.
- The free IP function is effective only when the port access control mode is **auto**.
- The maximum number of freely accessible network segments is 4.

Related commands: **display dot1x**.

Examples

Configure 192.168.0.0 as a freely accessible network segment.

```
<Sysname> system-view
[Sysname] dot1x free-ip 192.168.0.0 24
```

dot1x timer ead-timeout

Syntax

dot1x timer ead-timeout *ead-timeout-value*

undo dot1x timer ead-timeout

View

System view

Default Level

2: System level

Parameters

ead-timeout-value: EAD rule timeout time, in the range 1 minute to 1440 minutes.

Description

Use the **dot1x timer ead-timeout** command to set the EAD rule timeout time.

Use the **undo dot1x timer ead-timeout** command to restore the default.

By default, the timeout time is 30 minutes.

Related commands: **display dot1x**.

Examples

Set the EAD rule timeout time to 5 minutes.

```
<Sysname> system-view
[Sysname] dot1x timer ead-timeout 5
```

dot1x url

Syntax

dot1x url *url-string*

undo dot1x [*url-string*]

View

System view

Default Level

2: System level

Parameters

url-string: Redirect URL, a case-sensitive string of 1 to 64 characters in the format http://string/.

Description

Use the **dot1x url** command to configure a redirect URL. After a redirect URL is configured, when a user uses a Web browser to access networks other than the free IP, the device will redirect the user to the redirect URL.

Use the **undo dot1x url** command to remove the redirect URL.

By default, no redirect URL is defined.

Note that:

- The redirect URL and the free IP must be in the same network segment; otherwise, the URL may be inaccessible.
- You can configure the **dot1x url** command for more than once but only the last one takes effect.

Related commands: **display dot1x**, **dot1x free-ip**.

Examples

Configure the redirect URL as http://192.168.0.1.

```
<Sysname> system-view
[Sysname] dot1x url http://192.168.0.1
```

6 HABP Configuration Commands

HABP Configuration Commands

display habp

Syntax

display habp

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display habp** command to display HABP configuration information.

Examples

Display HABP configuration information.

```
<Sysname> display habp
Global HABP information:
   HABP Mode: Server
   Sending HABP request packets every 20 seconds
   Bypass VLAN: 2
```

Table 6-1 display habp command output description

Field	Description
HABP Mode	HABP mode of the current device, server or client
Sending HABP request packets every 20 seconds	Interval to send HABP request packets
Bypass VLAN	ID of the VLAN in which HABP packets are transmitted

display habp table

Syntax

display habp table

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display habp table** command to display HABP MAC address table entries.

Examples

Display HABP MAC address table entries.

```
<Sysname> display habp table
MAC           Holdtime  Receive Port
001f-3c00-0030  53       Ethernet1/1
```

Table 6-2 display habp table command output description

Field	Description
MAC	MAC address
Holdtime	Lifetime of an entry in seconds. The initial value is three times of the interval to send HABP request packets. An entry will age out if it is not updated during the period.
Receive Port	Port that learned the MAC address

display habp traffic

Syntax

display habp traffic

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display habp traffic** command to display HABP packet statistics.

Examples

Display HABP packet statistics.

```
<Sysname> display habp traffic
HABP counters :
   Packets output: 0, Input: 0
   ID error: 0, Type error: 0, Version error: 0
   Sent failed: 0
```

Table 6-3 display habp traffic command output description

Field	Description
Packets output	Number of HABP packets sent
Input	Number of HABP packets received
ID error	Number of packets with an incorrect ID
Type error	Number of packets with an incorrect type
Version error	Number of packets with an incorrect version number
Sent failed	Number of packets failed to be sent

habp enable

Syntax

habp enable

undo habp enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **habp enable** command to enable HABP.

Use the **undo habp enable** command to disable HABP.

By default, HABP is enabled.

HABP is required when and only when the cluster function and 802.1X (or MAC authentication) are enabled on the device.

Examples

Enable HABP.

```
<Sysname> system-view
[Sysname] habp enable
```

habp server vlan

Syntax

habp server vlan *vlan-id*

undo habp server

View

System view

Default Level

2: System level

Parameters

vlan-id: ID of the VLAN in which HABP packets are to be transmitted, in the range 1 to 4094.

Description

Use the **habp server vlan** command to configure HABP to work in server mode and specify the VLAN in which HABP packets are to be transmitted.

Use the **undo habp server vlan** command to configure HABP to work in the default mode.

By default, HABP works in client mode.

Examples

Configure HABP to work in server mode and specify the VLAN for HABP packets as VLAN 2.

```
<Sysname> system-view
[Sysname] habp server vlan 2
```

habp timer

Syntax

habp timer *interval*

undo habp timer

View

System view

Default Level

2: System level

Parameters

interval: Interval (in seconds) to send HABP request packets, in the range 5 to 600.

Description

Use the **habp timer** command to set the interval to send HABP request packets.

Use the **undo habp timer** command to restore the default.

The default interval is 20 seconds.

This command is required only on the HABP server.

Examples

Set the interval to send HABP request packets to 50 seconds.

```
<Sysname> system-view
[Sysname] habp timer 50
```

7 MAC Authentication Configuration Commands

MAC Authentication Configuration Commands

display mac-authentication

Syntax

display mac-authentication [**interface** *interface-list*]

View

Any view

Default Level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port. With an interface range, the end interface number and the start interface number must be of the same type and the former must be greater than the latter.

Description

Use the **display mac-authentication** command to display global MAC authentication information or MAC authentication information about specified ports.

Examples

Display global MAC authentication information.

```
<Sysname> display mac-authentication
MAC address authentication is enabled.
User name format is MAC address, like xxxxxxxxxxxx
 Fixed username:mac
 Fixed password:not configured
        Offline detect period is 300s
        Quiet period is 60s.
        Server response timeout value is 100s
        the max allowed user number is 1024 per slot
        Current user number amounts to 0
        Current domain: not configured, use default domain

Silent Mac User info:
       MAC Addr            From Port         Port Index
```

```
GigabitEthernet1/0/1 is link-up
  MAC address authentication is enabled
  Authenticate success: 0, failed: 0
  Current online user number is 0
MAC Addr       Authenticate state         Auth Index
```

……(part of the output omitted)

Table 7-1 display mac-authentication command output description

Field	Description
MAC address authentication is enabled	Whether MAC authentication is enabled
User name format is MAC address, like xxxxxxxxxxxx	The username is in the format of an MAC address without hyphens, like xxxxxxxxxxxx. If the username format is configured as MCA address with hyphens, “like xx-xx-xx-xx-xx-xx” will be displayed.
Fixed username:	Fixed username
Fixed password:	Password of the fixed username
Offline detect period	Setting of the offline detect timer
Quiet period	Setting of the quiet timer
Server response timeout value	Setting of the server timeout timer
the max allowed user number	Maximum number of users each slot in the device supports
Current user number amounts to	Number of online users
Current domain: not configured, use default domain	Currently used ISP domain
Silent Mac User info	Information about silent MAC addresses
GigabitEthernet1/0/1 is link-up	Status of the link on port GigabitEthernet 1/0/1
MAC address authentication is enabled	Whether MAC authentication is enabled on port GigabitEthernet 1/0/1
Authenticate success: 0, failed: 0	MAC authentication statistics, including the number of successful authentication attempts and that of unsuccessful authentication attempts
Current online user number	Number of online users on the port
MAC Addr	Online user MAC address
Authenticate state	User status. Possible values are: • CONNECTING: The user is logging in. • SUCCESS: The user has passed the authentication. • FAILURE: The user failed the authentication. • LOGOFF: The user has logged off.
Auth Index	Authenticator Index

mac-authentication

Syntax

In system view:

mac-authentication [**interface** *interface-list*]

undo mac-authentication [**interface** *interface-list*]

In Ethernet interface view:

mac-authentication

undo mac-authentication

View

System view, Ethernet interface view

Default Level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description

Use the **mac-authentication** command to enable MAC authentication globally or for one or more ports.

Use the **undo mac-authentication** command to disable MAC authentication globally or for one or more ports.

By default, MAC authentication is neither enabled globally nor enabled on any port.

Note that:

- In system view, if you provide the *interface-list* argument, the command enables MAC authentication for the specified ports; otherwise, the command enables MAC authentication globally. In Ethernet interface view, the command enables MAC authentication for the port because the *interface-list* argument is not available.
- You can enable MAC authentication for ports before enabling it globally. However, MAC authentication begins to function only after you also enable it globally.
- You can configure MAC authentication parameters globally or for specified ports either before or after enabling MAC authentication. If no MAC authentication parameters are configured when MAC authentication takes effect, the default values are used.

Examples

Enable MAC authentication globally.

```
<Sysname> system-view
[Sysname] mac-authentication
Mac-auth is enabled globally.
```

Enable MAC authentication for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] mac-authentication interface GigabitEthernet 1/0/1
Mac-auth is enabled on port GigabitEthernet1/0/1.
```

Or

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication
Mac-auth is enabled on port GigabitEthernet1/0/1.
```

mac-authentication domain

Syntax

mac-authentication domain *isp-name*

undo mac-authentication domain

View

System view

Default Level

2: System level

Parameters

isp-name: ISP domain name, a case-insensitive string of 1 to 24 characters that cannot contain any forward slash (/), colon (:), asterisk (*), question mark (?), less-than sign (<), greater-than sign (>), or @.

Description

Use the **mac-authentication domain** command to specify the ISP domain for MAC authentication.

Use the **undo mac-authentication domain** command to restore the default.

By default, the default ISP domain is used for MAC authentication users. For information about the default ISP domain, refer to the **domain default enable** command in *AAA Commands* of the *Security Volume*.

Examples

Specify the ISP domain for MAC authentication as domain1.

```
<Sysname> system-view
[Sysname] mac-authentication domain domain1
```

mac-authentication timer

Syntax

mac-authentication timer { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **server-timeout** }

View

System view

Default Level

2: System level

Parameters

offline-detect *offline-detect-value*: Specifies the offline detect interval, in the range 60 to 65,535 seconds.

quiet *quiet-value*: Specifies the quiet period, in the range 1 to 3,600 seconds.

server-timeout *server-timeout-value*: Specifies the server timeout period, in the range 100 to 300 seconds.

Description

Use the **mac-authentication timer** command to set the MAC authentication timers.

Use the **undo mac-authentication timer** command to restore the defaults.

By default, the offline detect interval is 300 seconds, the quiet period is 60 seconds, and the server timeout period is 100 seconds.

The following timers function in the process of MAC authentication:

- Offline detect timer: This timer sets the idle timeout interval for users. If no packet is received from a user over two consecutive timeout intervals, the system disconnects the user connection and notifies the RADIUS server.
- Quiet timer: Whenever a user fails MAC authentication, the device does not perform MAC authentication of the user during such a period.
- Server timeout timer: During authentication of a user, if the device receives no response from the RADIUS server in this period, it assumes that its connection to the RADIUS server has timed out and forbids the user from accessing the network.

Related commands: **display mac-authentication**.

Examples

Set the server timeout timer to 150 seconds.

```
<Sysname> system-view
[Sysname] mac-authentication timer server-timeout 150
```

mac-authentication user-name-format

Syntax

mac-authentication user-name-format { **fixed** [**account** *name*] [**password** { **cipher** | **simple** } *password*] | **mac-address** [**with-hyphen** | **without-hyphen**] }

undo mac-authentication user-name-format

View

System view

Default Level

2: System level

Parameters

fixed: Uses the MAC authentication username type of fixed username.

account *name*: Specifies the fixed username. The *name* argument is a case-insensitive string of 1 to 55 characters and defaults to mac.

password { **cipher** | **simple** } *password*: Specifies the password for the fixed username. Specify the **cipher** keyword to display the password in cipher text or the **simple** keyword to display the password in plain text. In the former case, the password can be either a string of 1 to 63 characters in plain text or a string of 24 or 88 characters in cipher text. In the latter case, the password must be a string of 1 to 63 characters in plain text.

mac-address: Uses the source MAC address of a user as the username for authentication.

with-hyphen: Indicates that the MAC address must include "-", like xx-xx-xx-xx-xx-xx. The letters in the address must be in lower case.

without-hyphen: Indicates that the MAC address must not include "-", like xxxxxxxxxxxx. The letters in the address must be in lower case.

Description

Use the **mac-authentication user-name-format** command to configure the MAC authentication username type and, if the type of fixed username is used, the username and password for MAC authentication.

Use the **undo mac-authentication user-name-format** command to restore the default.

By default, each user's source MAC address is used as the username and password for MAC authentication, with "-" in the MAC address.

Note that:

- When the type of MAC address is used, each user's source MAC address is used as both the username and password for MAC authentication.
- In cipher display mode, a password in plain text with no more than 16 characters will be encrypted into a password in cipher text with 24 characters, and a password in plain text with 16 to 63 characters will be encrypted into a password in cipher text with 88 characters. For a password with 24 characters, if it can be decrypted by the system, it will be treated as a cipher-text one; otherwise, it will be treated as a plain-text one.

Related commands: **display mac-authentication**.

Examples

Configure the username for MAC authentication as **abc**, and the password displayed in plain text as **xyz**.

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format fixed account abc password simple xyz
```

reset mac-authentication statistics

Syntax

reset mac-authentication statistics [**interface** *interface-list*]

View

User view

Default Level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description

Use the **reset mac-authentication statistics** command to clear MAC authentication statistics.

Note that:

- If you do not specify the *interface-list* argument, the command clears the global MAC authentication statistics and the MAC authentication statistics on all ports.
- If you specify the *interface-list* argument, the command clears the MAC authentication statistics on the specified ports.

Related commands: **display mac-authentication**.

Examples

Clear MAC authentication statistics on GigabitEthernet 1/0/1.

```
<Sysname> reset mac-authentication statistics interface GigabitEthernet 1/0/1
```

8 Port Security Configuration Commands

Port Security Configuration Commands

display port-security

Syntax

display port-security [**interface** *interface-list*]

View

Any view

Default Level

2: System level

Parameters

interface-list: Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> means that you can specify up to 10 port or port ranges. The starting port and ending port of a port range must be of the same type and the ending port number must be greater than the starting port number.

Description

Use the **display port-security** command to display port security configuration information, operation information, and statistics about one or more specified ports or all ports.

Related commands: **port-security enable**, **port-security port-mode**, **port-security ntk-mode**, **port-security intrusion-mode**, **port-security max-mac-count**, **port-security mac-address security**, **port-security authorization ignore**, **port-security oui**, **port-security trap**.

Examples

Display port security configuration information, operation information, and statistics about all ports.

```
<Sysname> display port-security
 Equipment port-security is enabled
 AddressLearn trap is enabled
 Intrusion trap is enabled
 Dot1x logon trap is enabled
 Dot1x logoff trap is enabled
 Dot1x logfailure trap is enabled
 RALM logon trap is enabled
 RALM logoff trap is enabled
 RALM logfailure trap is enabled
 Disableport Timeout: 20s
 OUI value:
   Index is 1,  OUI value is 000d1a
```

```
  Index is 2,  OUI value is 003c12

GigabitEthernet1/0/1 is link-down
   Port mode is UserloginWithOUI
   NeedtoKnow mode is needtoknowonly
   Intrusion mode is disableport
   Max MAC address number is 50
   Stored MAC address number is 0
   Authorization is ignored
GigabitEthernet1/0/2 is link-down
   Port mode is noRestriction
   NeedtoKnow mode is disabled
   Intrusion mode is no action
   Max MAC address number is not configured
   Stored MAC address number is 0
   Authorization is permitted
```

Table 8-1 display port-security command output description

Field	Description
Equipment port-security is enabled	Port security is enabled.
AddressLearn trap is enabled	Address learning trap is enabled.
Intrusion trap is enabled	Intrusion protection trap is enabled.
Dot1x logon trap is enabled	802.1X logon trap is enabled.
Dot1x logoff trap is enabled	802.1X logoff trap is enabled.
Dot1x logfailure is enabled	802.1X authentication failure trap is enabled.
RALM logon trap is enabled	MAC authentication success trap is enabled.
RALM logoff trap is enabled	MAC authenticated user logoff trap is enabled.
RALM logfailure trap is enabled	MAC authentication failure trap is enabled.
Disableport Timeout	Silence timeout of the port, in seconds.
OUI value	24-bit OUI value
Index	OUI index
Port mode is UserloginWithOUI	The port security mode is UserloginWithOUI.
NeedtoKnow mode is needtoknowonly	The NTK mode is needtoknowonly.
Intrusion mode is disableport	Intrusion protection action is set to **disableport**.
Max MAC address number	Maximum number of secure MAC addresses allowed on the port
Stored MAC address number	Number of MAC addresses stored
Authorization is ignored	Authorization information from the server is ignored. By default, the information takes effect and this field is displayed as “Authorization is permitted.”

display port-security mac-address block

Syntax

display port-security mac-address block [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

View

Any view

Default Level

2: System level

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies a VLAN by its number, which is in the range 1 to 4094.

count: Displays only the count of the blocked MAC addresses.

Description

Use the **display port-security mac-address block** command to display information about blocked MAC addresses.

With no keyword or argument specified, the command displays information about all blocked MAC addresses.

Related commands: **port-security intrusion-mode**.

Examples

Display information about all blocked MAC addresses.

```
<Sysname> display port-security mac-address block
MAC ADDR           From Port               VLAN ID
0002-0002-0002     GigabitEthernet1/0/1            1
000d-88f8-0577     GigabitEthernet1/0/1            1

  --- On slot 2, 2 mac address(es) found ---
  ---  2 mac address(es) found  ---
```

Display the count of all blocked MAC addresses.

```
<Sysname> display port-security mac-address block count
 --- On slot 2, 2 mac address(es) found ---
 --- 2 mac address(es) found ---
```

Display information about all blocked MAC addresses in VLAN 1.

```
<Sysname> display port-security mac-address block vlan 1
MAC ADDR           From Port               VLAN ID
0002-0002-0002     GigabitEthernet1/0/1            1
000d-88f8-0577     GigabitEthernet1/0/1            1

 --- On slot 2,2 mac address(es) found  ---
 --- 2 mac address(es) found ---
```

Display information about all blocked MAC addresses of port GigabitEthernet 1/0/1.

```
<Sysname> display port-security mac-address block interface GigabitEthernet1/0/1
MAC ADDR           From Port               VLAN ID
000d-88f8-0577     GigabitEthernet1/0/1            1

--- On slot 2, 1 mac address(es) found ---
  ---  1 mac address(es) found  ---
```

Display information about all blocked MAC addresses of port GigabitEthernet 1/0/1 in VLAN 1.

```
<Sysname> display port-security mac-address block interface GigabitEthernet 1/0/1 vlan 1
MAC ADDR           From Port               VLAN ID
000d-88f8-0577     GigabitEthernet1/0/1            1

--- On slot 2, 1 mac address(es) found ---
  ---  1 mac address(es) found  ---
```

Table 8-2 display port-security mac-address block command output description

Field	Description
MAC ADDR	Blocked MAC address
From Port	Port having received frames with the blocked MAC address being the source address
VLAN ID	ID of the VLAN to which the port belongs
2 mac address(es) found	Number of blocked MAC addresses

display port-security mac-address security

Syntax

display port-security mac-address security [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

View

Any view

Default Level

2: System level

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies a VLAN by its number, which is in the range 1 to 4094.

count: Displays only the count of the secure MAC addresses.

Description

Use the **display port-security mac-address security** command to display information about secure MAC addresses.

With no keyword or argument specified, the command displays information about all secure MAC addresses.

Related commands: **port-security mac-address security**.

Examples

Display information about all secure MAC addresses.

```
<Sysname> display port-security mac-address security
MAC ADDR       VLAN ID   STATE        PORT INDEX            AGING TIME(s)
0002-0002-0002  1        Security      GigabitEthernet1/0/1    NOAGED
000d-88f8-0577  1        Security      GigabitEthernet1/0/1    NOAGED

  ---  2 mac address(es) found  ---
```

Display only the count of the secure MAC addresses.

```
<Sysname> display port-security mac-address count
 2 mac address(es) found
```

Display information about secure MAC addresses in a specified VLAN.

```
<Sysname> display port-security mac-address security vlan 1
MAC ADDR       VLAN ID   STATE        PORT INDEX            AGING TIME(s)
0002-0002-0002  1        Security      GigabitEthernet1/0/1    NOAGED
000d-88f8-0577  1        Security      GigabitEthernet1/0/1    NOAGED

  ---  2 mac address(es) found  ---
```

Display information about secure MAC addresses on the specified port.

```
<Sysname> display port-security mac-address security interface GigabitEthernet1/0/1
MAC ADDR       VLAN ID   STATE        PORT INDEX            AGING TIME(s)
000d-88f8-0577  1        Security      GigabitEthernet1/0/1    NOAGED

  ---  1 mac address(es) found  ---
```

Display information about secure MAC addresses that are on the specified port and in the specified VLAN.

```
<Sysname> display port-security mac-address security interface GigabitEthernet 1/0/1 vlan
1
MAC ADDR       VLAN ID   STATE        PORT INDEX            AGING TIME(s)
000d-88f8-0577  1        Security      GigabitEthernet1/0/1    NOAGED

  ---  1 mac address(es) found  ---
```

Table 8-3 display port-security mac-address command output description

Field	Description
MAC ADDR	Secure MAC address
VLAN ID	VLAN to which the port belongs
STATE	Type of the MAC address added
PORT INDEX	Port to which the secure MAC address belongs
AGING TIME(s)	Period of time before the secure MAC address ages out

Field	Description
xxx mac address(es) found	Number of secure MAC addresses stored

port-security authorization ignore

Syntax

port-security authorization ignore

undo port-security authorization ignore

View

Layer 2 Ethernet interface view

Default Level

2: System level

Parameters

None

Description

Use the **port-security authorization ignore** command to configure a port to ignore the authorization information from the RADIUS server.

Use the **undo port-security port-mode ignore** command to restore the default.

By default, a port uses the authorization information from the RADIUS server.

After a user passes RADIUS authentication, the RADIUS server performs authorization based on the authorization attributes configured for the user's account. For example, it may assign a VLAN.

Related commands: **display port-security**.

Examples

Configure port GigabitEthernet 1/0/1 to ignore the authorization information from the RADIUS server.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security authorization ignore
```

port-security enable

Syntax

port-security enable

undo port-security enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **port-security enable** command to enable port security.

Use the **undo port-security enable** command to disable port security.

By default, port security is disabled.

Note that:

1) Port security cannot be enabled when 802.1X or MAC authentication is enabled globally.
2) Enabling port security resets the following configurations on a port to the defaults bracketed, making them dependent completely on the port security mode:

- 802.1X (disabled), port access control method (**macbased**), and port access control mode (**auto**)
- MAC authentication (disabled)

3) Disabling port security resets the following configurations on a port to the defaults bracketed:

- Port security mode (noRestrictions)
- 802.1X (disabled), port access control method (**macbased**), and port access control mode (**auto**)
- MAC authentication (disabled)

4) Port security cannot be disabled if there is any user present on a port.

Related commands: **display port-security**, **dot1x**, **dot1x port-method**, **dot1x port-control** in *802.1X Commands* of the *Security Volume*, **mac-authentication** in *MAC Authentication Commands* of the *Security Volume*.

Examples

Enable port security.

```
<Sysname> system-view
[Sysname] port-security enable
```

port-security intrusion-mode

Syntax

port-security intrusion-mode { **blockmac** | **disableport** | **disableport-temporarily** }

undo port-security intrusion-mode

View

Layer 2 Ethernet interface view

Default Level

2: System level

Parameters

blockmac: Adds the source MAC addresses of illegal frames to the blocked MAC address list and discards frames with blocked source MAC addresses. A blocked MAC address is restored to normal after being blocked for three minutes, which is fixed and cannot be changed. You can use the **display port-security mac-address block** command to view the blocked MAC address list.

disableport: Disables the port permanently upon detecting an illegal frame received on the port.

disableport-temporarily: Disables the port for a specified period of time whenever it receives an illegal frame. Use the **port-security timer disableport** command to set the period.

Description

Use the **port-security intrusion-mode** command to configure the intrusion protection feature, so that the interface performs configured security policies in response to received illegal packets.

Use the **undo port-security intrusion-mode** command to restore the default.

By default, intrusion protection is disabled.

You can use the **undo shutdown** command to restore the connection of the port.

Related commands: **display port-security**, **display port-security mac-address block**, **port-security timer disableport**.

Examples

Configure port GigabitEthernet 1/0/1 to block the source MAC addresses of illegal frames after intrusion protection is triggered.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
```

port-security mac-address security

Syntax

In Layer 2 Ethernet interface view:

port-security mac-address security *mac-address* **vlan** *vlan-id*

In system view:

port-security mac-address security *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

undo port-security mac-address security [[*mac-address* [**interface** *interface-type interface-number*]] **vlan** *vlan-id*]

View

Layer 2 Ethernet Interface view, system view

Default Level

2: System level

Parameters

mac-address: Secure MAC address, in the H-H-H format.

interface *interface-type interface-number*: Specifies a Layer 2 Ethernet port by its type and number.

vlan-id: ID of the VLAN to which the secure MAC address belongs, in the range 1 to 4094.

Description

Use the **port-security mac-address security** command to add a secure MAC address.

Use the **undo port-security mac-address security** command to remove specified secure MAC addresses.

By default, no secure MAC address is configured.

Note that:

- The port must belong to the specified VLAN.
- You can configure a secure MAC address only if port security is enabled and the specified port operates in autoLearn mode.
- The **undo port-security mac-address security** command can be used in system view only.

Related commands: **display port-security**.

Examples

Enable port security, set the port security mode of port GigabitEthernet 1/0/1 to autoLearn, and add a secure MAC address of 0001-0001-0002 (belonging to VLAN 10) for port GigabitEthernet 1/0/1 in system view.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
[Sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] port-security mac-address security 0001-0001-0002 interface gigabitethernet 1/0/1
vlan 10
```

Enable port security, set the port security mode of port GigabitEthernet 1/0/1 to autoLearn, and add a secure MAC address of 0001-0002-0003 (belonging to VLAN 4) for port GigabitEthernet 1/0/1 in interface view.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
[Sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
[Sysname-GigabitEthernet1/0/1] port-security mac-address security 0001-0002-0003 vlan 4
```

port-security max-mac-count

Syntax

port-security max-mac-count *count-value*

undo port-security max-mac-count

View

Ethernet interface view

Default Level

2: System level

Parameters

count-value: Maximum number of secure MAC addresses allowed on the port, ranging 1 to 1,024.

Description

Use the **port-security max-mac-count** command to set the maximum number of secure MAC addresses allowed on the port.

Use the **undo port-security max-mac-count** command to restore the default setting.

By default, the maximum number of secure MAC addresses is not limited.

Note that:

- You cannot change the maximum number of secure MAC addresses for a port working in the **autoLearn** mode.
- The maximum number of secure MAC addresses allowed on a port does not include or limit that of the static MAC addresses manually configured.
- The maximum number of secure MAC addresses allowed on a port must not be less than the number of MAC addresses stored on the port.

Related commands: **display port-security**.

Examples

Set the maximum number of secure MAC addresses allowed on port GigabitEthernet 1/0/1 to 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
```

port-security ntk-mode

Syntax

port-security ntk-mode { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkonly** }

undo port-security ntk-mode

View

Ethernet interface view

Default Level

2: System level

Parameters

ntk-withbroadcasts: Sends only frames destined for authenticated MAC addresses or the broadcast address.

ntk-withmulticasts: Sends only frames destined for authenticated MAC addresses, multicast addresses, or the broadcast address.

ntkonly: Sends only frames destined for authenticated MAC addresses.

Description

Use the **port-security ntk-mode** command to configure the NTK feature.

Use the **undo port-security ntk-mode** command to restore the default.

Be default, NTK is disabled on a port and all frames are allowed to be sent.

The need to know (NTK) feature checks the destination MAC addresses in outbound frames to allow frames to be sent to only devices passing authentication, thus preventing illegal devices from intercepting network traffic.

Related commands: **display port-security**.

Examples

Set the NTK mode of port GigabitEthernet 1/0/1 to **ntkonly**, allowing the port to forward received packets to only devices passing authentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

port-security oui

Syntax

port-security oui *oui-value* **index** *index-value*

undo port-security oui index *index-value*

View

System view

Default Level

2: System level

Parameters

oui-value: Organizationally unique identifier (OUI) string, a 48-bit MAC address in the H-H-H format. The system automatically uses only the 24 high-order bits as the OUI value.

index-value: OUI index, in the range 1 to 16.

Description

Use the **port-security oui** command to configure an OUI value for user authentication. This value is used when the port security mode is UserLoginWithOUI.

Use the **undo port-security oui** command to delete an OUI value with the specified OUI index.

By default, no OUI value is configured.

Note that an OUI value configured by using the **port-security oui** command takes effect only when the security mode is userLoginWithOUI.

Related commands: **display port-security**.

Examples

Configure an OUI value of 000d2a, setting the index to 4.

```
<Sysname> system-view
[Sysname] port-security oui 000d-2a10-0033 index 4
```

port-security port-mode

Syntax

port-security port-mode { **autolearn** | **mac-authentication** | **mac-else-userlogin-secure** | **mac-else-userlogin-secure-ext** | **secure** | **userlogin** | **userlogin-secure** | **userlogin-secure-ext** | **userlogin-secure-or-mac** | **userlogin-secure-or-mac-ext** | **userlogin-withoui** }

undo port-security port-mode

View

Interface view

Default Level

2: System level

Parameters

autolearn: Operates in autoLearn mode.

mac-authentication: Operates in macAddressWithRadius mode.

mac-else-userlogin-secure: Operates in macAddressElseUserLoginSecure mode.

mac-else-userlogin-secure-ext: Operates in macAddressElseUserLoginSecureExt mode.

secure: Operates in secure mode.

userlogin: Operates in userLogin mode.

userlogin-secure: Operates in userLoginSecure mode.

userlogin-secure-ext: Operates in userLoginSecureExt mode.

userlogin-secure-or-mac: Operates in macAddressOrUserLoginSecure mode.

userlogin-secure-or-mac-ext: Operates in macAddressOrUserLoginSecureExt mode.

userlogin-withoui: Operates in userLoginWithOUI mode.

Description

Use the **port-security port-mode** command to set the port security mode of a port.

Use the **undo port-security port-mode** command to restore the default.

By default, a port operates in noRestrictions mode, where port security does not take effect.

Note that:

- Configuration of port security mode on a port is mutually exclusive with the configuration of 802.1X authentication, port access control method, port access control mode, and MAC authentication on the port.
- With port security enabled, you can change the port security mode of a port only when the port is operating in noRestrictions mode, the default mode. You can use the **undo port-security port-mode** command to restore the default port security mode.
- Before configuring the port security mode to autoLearn, be sure to configure the maximum number of secure MAC addresses allowed on the port by using the **port-security max-mac-count** command.
- You cannot change the port security mode of a port with users online.

Related commands: **display port-security**.

Examples

Enable port security and configure the port security mode of port GigabitEthernet 1/0/1 as secure.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security port-mode secure
```

Change the port security mode of port GigabitEthernet 1/0/1 to userLogin.

```
[Sysname-GigabitEthernet1/0/1] undo port-security port-mode
[Sysname-GigabitEthernet1/0/1] port-security port-mode userlogin
```

port-security timer disableport

Syntax

port-security timer disableport *time-value*

undo port-security timer disableport

View

System view

Default Level

2: System level

Parameters

time-value: Silence timeout during which the port remains disabled, in seconds. It ranges from 20 to 300.

Description

Use the **port-security timer disableport** command to set the silence timeout during which the port remains disabled.

Use the **undo port-security timer disableport** command to restore the default.

By default, the silence timeout is 20 seconds.

If you configure the intrusion protection policy as disabling the port temporarily whenever it receives an illegal frame, you can use this command to set the silence period.

Related commands: **display port-security**.

Examples

Configure the intrusion protection policy as disabling the port temporarily whenever it receives an illegal frame and set the silence timeout to 30 seconds.

```
<Sysname> system-view
[Sysname] port-security timer disableport 30
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

port-security trap

Syntax

port-security trap { **addresslearned** | **dot1xlogfailure** | **dot1xlogoff** | **dot1xlogon** | **intrusion** | **ralmlogfailure** | **ralmlogoff** | **ralmlogon** }

undo port-security trap { **addresslearned** | **dot1xlogfailure** | **dot1xlogoff** | **dot1xlogon** | **intrusion** | **ralmlogfailure** | **ralmlogoff** | **ralmlogon** }

View

System view

Default Level

2: System level

Parameters

addresslearned: Address learning trap. When enabled, this function allows the system to send a trap message when a port learns a new MAC address.

dot1xlogfailure: Trap for 802.1X authentication failure.

dot1xlogon: Trap for successful 802.1X authentication.

dot1xlogoff: Trap for 802.1X user logoff events.

intrusion: Trap for illegal frames.

ralmlogfailure: Trap for MAC authentication failure.

ralmlogoff: Trap for MAC authentication user logoff events.

ralmlogon: Trap for successful MAC authentication.

 **Note**

RALM (RADIUS Authenticated Login using MAC-address) means RADIUS authentication based on MAC address.

Description

Use the **port-security trap** command to enable port security traps.

Use the **undo port-security trap** command to disable port security traps.

By default, no port security trap is enabled.

This command involves the trap feature. With the trap feature, a device can send trap information upon receiving packets that result from, for example, intrusion, abnormal login, or logout operations, allowing you to monitor operations of interest.

Related commands: **display port-security**.

Examples

Enable address learning trap.

```
<Sysname> system-view
[Sysname] port-security trap addresslearned
```

9 IP Source Guard Configuration Commands

IP Source Guard Configuration Commands

display ip check source

Syntax

display ip check source [**interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address*]

View

Any view

Default Level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the dynamic bindings of the interface specified by its type and number.

ip-address *ip-address*: Displays the dynamic bindings of an IP address.

mac-address *mac-address*: Displays the dynamic bindings of an MAC address (in the format of H-H-H).

Description

Use the **display ip check source** command to display dynamic bindings.

With no options specified, the command displays the dynamic bindings of all interfaces.

Related commands: **ip check source**.

Examples

Display all dynamic bindings.

```
<Sysname> display ip check source
Total entries found: 2
  MAC               IP         Vlan      Port               Status
  040a-0000-4000     10.1.0.9    2         GigabitEthernet1/0/1  DHCP-SNP
  040a-0000-2000     10.1.0.7    2         GigabitEthernet1/0/1  DHCP-SNP
```

Table 9-1 display ip check source command output description

Field	Description
Total entries found	Total number of found entries
MAC	MAC address of the dynamic binding. N/A means that no MAC address is bound in the entry.
IP	IP address of the dynamic binding. N/A means that no IP address is bound in the entry.
Vlan	VLAN to which the obtained binding entry belongs. N/A means that no VLAN is bound in the entry.
Port	Port to which the dynamic binding entry is applied
Status	Type of dynamically obtaining the binding entry

display user-bind

Syntax

display user-bind [**interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address*]

View

Any view

Default Level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the static bindings of the interface specified by its type and number.

ip-address *ip-address*: Displays the static bindings of an IP address.

mac-address *mac-address*: Displays the static bindings of an MAC address (in the format of H-H-H).

Description

Use the **display user-bind** command to display static bindings.

With no options specified, the command displays static bindings of all interfaces.

Related commands: **user-bind**.

Examples

Display all static bindings.

```
<Sysname> display user-bind
Total entries found: 4
 MAC             IP             Vlan   Port                      Status
 N/A             1.1.1.1         N/A   GigabitEthernet1/0/1        Static
 0001-0001-0001   2.2.2.2         200   GigabitEthernet1/0/1        Static
 0003-0003-0003   N/A            N/A   GigabitEthernet1/0/2        Static
 0004-0004-0004   4.4.4.4         N/A   GigabitEthernet1/0/2        Static
```

Table 9-2 display user-bind command output description

Field	Description
Total entries found	Total number of found entries
MAC	MAC address of the binding. N/A means that no MAC address is bound in the entry.
IP	IP address of the binding. N/A means that no IP address is bound in the entry.
Vlan	VLAN of the binding. N/A means that no VLAN is bound in the entry.
Port	Port of the binding
Status	Type of the binding. Static means that the binding is manually configured.

ip check source

Syntax

ip check source { **ip-address** | **ip-address mac-address** | **mac-address** }

undo ip check source

View

Ethernet interface view, VLAN interface view

Default Level

2: System level

Parameters

ip-address: Specifies to bind source IP address to the port.

ip-address mac-address: Specifies to bind source IP address and MAC address to the port.

mac-address: Specifies to bind source MAC address to the port.

Description

Use the **ip check source** command to configure the dynamic binding function on a port.

Use the **undo ip check source** command to restore the default.

By default, the dynamic binding function is disabled.

Note that:You cannot configure the dynamic binding function on a port that is in an aggregation group.

Related commands: **display ip check source**.

Examples

Configure dynamic binding function on port GigabitEthernet1/0/1 to filter packets based on both source IP address and MAC address.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] ip check source ip-address mac-address
```

user-bind

Syntax

user-bind { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

undo user-bind { **ip-address** *ip-address* | **ip-address** *ip-address* **mac-address** *mac-address* | **mac-address** *mac-address* } [**vlan** *vlan-id*]

View

Layer-2 Ethernet interface view

Default Level

2: System level

Parameters

ip-address *ip-address*: Specifies the IP address for the static binding. The IP address can only be a Class A, Class B, or Class C address and can be neither 127.x.x.x nor 0.0.0.0.

mac-address *mac-address*: Specifies the MAC address for the static binding in the format of H-H-H. The MAC address cannot be all 0s, all Fs (a broadcast address), or a multicast address.

vlan *vlan-id*: Specifies the VLAN for the static binding. *vlan-id* is the ID of the VLAN to be bound, in the range 1 to 4094.

Description

Use the **user-bind** command to configure a static binding.

Use the **undo user-bind** command to delete a static binding.

By default, no static binding exists on a port.

Note that:

- The system does not support repeatedly configuring a binding entry to one port.
- For products supporting multi-port binding, a binding entry can be configured to multiple ports; for products that do not support multi-port binding, a binding entry can be configured to only one port.
- You cannot configure a static binding on a port that is in an aggregation group.

Related commands: **display user-bind**.

Examples

Configure a static binding on port GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] user-bind ip-address 192.168.0.1 mac-address 0001-0001-0001
```

10 SSH2.0 Configuration Commands

SSH2.0 Server Configuration Commands

display ssh server

Syntax

display ssh server { **session** | **status** }

View

Any view

Default Level

1: Monitor level

Parameters

session: Displays the session information of the SSH server.

status: Displays the status information of the SSH server.

Description

Use the **display ssh server** command on an SSH server to display SSH server status information or session information.

Related commands: **ssh server authentication-retries**, **ssh server rekey-interval**, **ssh server authentication-timeout**, **ssh server enable**, **ssh server compatible-ssh1x enable**.

 **Note**

This command is also available on an SFTP server.

Examples

Display the SSH server status information.

```
<Sysname> display ssh server status
 SSH Server: Disable
 SSH version : 1.99
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH authentication retries : 3 time(s)
 SFTP server: Disable
```

```
SFTP server Idle-Timeout: 10 minute(s)
```

Table 10-1 display ssh server status command output description

Field	Description
SSH Server	Whether the SSH server function is enabled
SSH version	SSH protocol version When the SSH supports SSH1, the protocol version is 1.99. Otherwise, the protocol version is 2.0.
SSH authentication-timeout	Authentication timeout period
SSH server key generating interval	SSH server key pair update interval
SSH authentication retries	Maximum number of SSH authentication attempts
SFTP server	Whether the SFTP server function is enabled
SFTP server Idle-Timeout	SFTP connection idle timeout period

Display the SSH server session information.

```
<Sysname> display ssh server session
 Conn   Ver   Encry    State        Retry    SerType  Username
 VTY 0  2.0   DES      Established   0       SFTP     client001
```

Table 10-2 display ssh server session command output description

Field	Description
Conn	Connected VTY channel
Ver	SSH server protocol version
Encry	Encryption algorithm
State	Status of the session, including: Init, Ver-exchange, Keys-exchange, Auth-request, Serv-request, Established, Disconnected
Retry	Number of authentication attempts
SerType	Service type (SFTP, Stelnet)
Username	Name of a user during login

display ssh user-information

Syntax

display ssh user-information [*username*]

View

Any view

Default Level

1: Monitor level

Parameters

username: SSH username, a string of 1 to 80 characters.

Description

Use the **display ssh user-information** command on an SSH server to display information about one or all SSH users.

With the *username* argument not specified, the command displays information about all SSH users.

Related commands: **ssh user**.

Note

This command is also available on an SFTP server.

Examples

Display information about all SSH users.

```
<Sysname> display ssh user-information
 Total ssh users : 2
 Username    Authentication-type   User-public-key-name    Service-type
 yemx        password              null                    stelnet|sftp
 test        publickey             pubkey                     sftp
```

Table 10-3 display ssh user-information command output description

Field	Description
Username	Name of the user
Authentication-type	Authentication method. If this field has a value of **password**, the next field will have a value of **null**.
User-public-key-name	Public key of the user
Service-type	Service type

ssh server authentication-retries

Syntax

ssh server authentication-retries *times*

undo ssh server authentication-retries

View

System view

Default Level

2: System level

Parameters

times: Maximum number of authentication attempts, in the range 1 to 5.

Description

Use the **ssh server authentication-retries** command to set the maximum number of SSH connection authentication attempts, which takes effect at next login.

Use the **undo ssh server authentication-retries** command to restore the default.

By default, the maximum number of SSH connection authentication attempts is 3.

Note that:

- Authentication will fail if the number of authentication attempts (including both publickey and password authentication) exceeds that specified in the **ssh server authentication-retries** command.
- If the authentication method of SSH users is **password-publickey**, the maximum number of SSH connection authentication attempts must be at least 2. This is because SSH2.0 users must pass both password and publickey authentication.

Related commands: **display ssh server**.

Examples

Set the maximum number of SSH connection authentication attempts to 4.

```
<Sysname> system-view
[Sysname] ssh server authentication-retries 4
```

ssh server authentication-timeout

Syntax

ssh server authentication-timeout *time-out-value*

undo ssh server authentication-timeout

View

System view

Default Level

2: System level

Parameters

time-out-value: Authentication timeout period in seconds, in the range 1 to 120.

Description

Use the **ssh server authentication-timeout** command to set the SSH user authentication timeout period on the SSH server.

Use the **undo ssh server authentication-timeout** command to restore the default.

By default, the authentication timeout period is 60 seconds.

Related commands: **display ssh server**.

Examples

Set the SSH user authentication timeout period to 10 seconds.

```
<Sysname> system-view
[Sysname] ssh server authentication-timeout 10
```

ssh server compatible-ssh1x enable

Syntax

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **ssh server compatible-ssh1x** command to enable the SSH server to work with SSH1 clients.

Use the **undo ssh server compatible-ssh1x** command to disable the SSH server from working with SSH1 clients.

By default, the SSH server can work with SSH1 clients.

This configuration takes effect only for users logging in after the configuration.

Related commands: **display ssh server**.

Examples

Enable the SSH server to work with SSH1 clients.

```
<Sysname> system-view
[Sysname] ssh server compatible-ssh1x enable
```

ssh server enable

Syntax

ssh server enable

undo ssh server enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **ssh server enable** command to enable SSH server.

Use the **undo ssh server enable** command to disable SSH server.

By default, SSH server is disabled.

Examples

Enable SSH server.

```
<Sysname> system-view
[Sysname] ssh server enable
```

ssh server rekey-interval

Syntax

ssh server rekey-interval *hours*

undo ssh server rekey-interval

View

System view

Default Level

2: System level

Parameters

hours: Server key pair update interval in hours, in the range 1 to 24.

Description

Use the **ssh server rekey-interval** command to set the interval for updating the RSA server key.

Use the **undo ssh server rekey-interval** command to remove the configuration.

By default, the update interval of the RSA server key is 0, that is, the RSA server key is not updated.

Related commands: **display ssh server**.

 **Caution**

- This command is only available to SSH users using SSH1 client software.
- The system does not update any DSA key pair periodically.

Examples

Set the RSA server key pair update interval to 3 hours.

```
<Sysname> system-view
```

```
[Sysname] ssh server rekey-interval 3
```

ssh user

Syntax

ssh user *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* }

ssh user *username* **service-type** { **all** | **sftp** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* **work-directory** *directory-name* }

undo ssh user *username*

View

System view

Default Level

2: System level

Parameters

username: SSH username, a case-sensitive string of 1 to 80 characters.

service-type: Specifies the service type of an SSH user, which can be one of the following:

- **all**: Specifies both secure Telnet and secure FTP.
- **sftp**: Specifies the service type as secure FTP.
- **stelnet**: Specifies the service type of secure Telnet.

authentication-type: Specifies the authentication method of an SSH user, which can be one the following:

- **password**: Performs password authentication.
- **any**: Performs either password authentication or publickey authentication.
- **password-publickey**: Specifies that SSH2 clients perform both password authentication and publickey authentication and that SSH1 clients perform either type of authentication.
- **publickey**: Performs publickey authentication.

assign publickey *keyname*: Assigns an existing public key to an SSH user. *keyname* indicates the name of the client public key and is a string of 1 to 64 characters.

work-directory *directory-name*: Specifies the working folder for an SFTP user. *directory-name* indicates the name of the working folder and is a string of 1 to 135 characters.

Description

Use the **ssh user** command to create an SSH user and specify the service type and authentication method.

Use the **undo ssh user** command to delete an SSH user.

Note that:

- For a publickey authentication user, you must configure the username and the public key on the device. For a password authentication user, you can configure the account information on either the device or the remote authentication server such as a RADIUS server.
- If you use the **ssh user** command to configure a public key for a user who has already had a public key, the new one overwrites the old one.

- Authentication method and public key configuration takes effect only for users logging in after the configuration.
- If an SFTP user has been assigned a public key, it is necessary to set a working folder for the user.
- The working folder of an SFTP user is subject to the user authentication method. For a user using only password authentication, the working folder is the AAA authorized one. For a user using only publickey authentication or using both the publickey and password authentication methods, the working folder is the one set by using the **ssh user** command.

Related commands: **display ssh user-information**.

Examples

Create an SSH user named **user1**, setting the service type as **sftp**, the authentication method as **publickey**, the work folder of the SFTP server as **flash**, and assigning a public key named **key1** to the user.

```
<Sysname> system-view
[Sysname] ssh user user1 service-type sftp authentication-type publickey assign publickey
key1 work-directory flash:
```

SSH2.0 Client Configuration Commands

display ssh client source

Syntax

display ssh client source

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ssh client source** command to display the source IP address or source interface currently set for the SSH client.

If neither source IP address nor source interface is specified for the SSH client, the system will prompt you to specify the source information.

Related commands: **ssh client source**.

Examples

Display the source IP address of the SSH client.

```
<Sysname> display ssh client source
The source IP address you specified is 192.168.0.1
```

display ssh server-info

Syntax

display ssh server-info

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ssh server-info** command on a client to display mappings between SSH servers and their host public keys saved on the client.

When an SSH client needs to authenticate the SSH server, it uses the locally saved public key of the server for the authentication. If the authentication fails, you can use this command to check the public key of the server saved on the client.

Related commands: **ssh client authentication server**.

Note

This command is also available on an SFTP client.

Examples

Display the mappings between host public keys and SSH servers saved on the client.

```
<Sysname> display ssh server-info
Server Name(IP)              Server public key name
_____________________________________________________
192.168.0.1                  abc_key01
192.168.0.2                  abc_key02
```

Table 10-4 display ssh server-info command output description

Field	Description
Server Name(IP)	Name or IP address of the server
Server public key name	Name of the host public key of the server

ssh client authentication server

Syntax

ssh client authentication server *server* **assign publickey** *keyname*

undo ssh client authentication server *server* **assign publickey**

View

System view

Default Level

2: System level

Parameters

server: IP address or name of the server, a string of 1 to 80 characters.

keyname: Name of the host public key of the server, a string of 1 to 64 characters.

Description

Use the **ssh client authentication server** command on a client to configure the host public key of the server so that the client can determine whether the server is trustworthy.

Use the **undo ssh authentication server** command to remove the configuration.

By default, the host public key of the server is not configured, and when logging into the server, the client uses the IP address or host name used for login as the public key name.

If the client does not support first authentication, it will reject unauthenticated servers. In this case, you need to configure the public keys of the servers and specify the mappings between public keys and servers on the client, so that the client uses the correct public key of a server to authenticate the server.

Note that the specified host public key of the server must already exist.

Related commands: **ssh client first-time enable**.

Examples

Configure the public key of the server with the IP address of 192.168.0.1 to be key1.

```
<Sysname> system-view
[Sysname] ssh client authentication server 192.168.0.1 assign publickey key1
```

ssh client first-time enable

Syntax

ssh client first-time e**nable**

undo ssh client first-time

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **ssh client first-time enable** command to enable the first authentication function.

Use the **undo ssh client first-time** command to disable the function.

By default, the function is enabled.

With first-time authentication, when an SSH client not configured with the server host public key accesses the server for the first time, the user can continue accessing the server, and save the host public key on the client. When accessing the server again, the client will use the saved server host public key to authenticate the server.

Without first-time authentication, a client not configured with the server host public key will deny to access the server. To access the server, a user must configure in advance the server host public key locally and specify the public key name for authentication.

Note that as the server may update its key pairs periodically, clients must obtain the most recent public keys of the server for successful authentication of the server.

Examples

Enable the first authentication function.

```
<Sysname> system-view
[Sysname] ssh client first-time enable
```

ssh client ipv6 source

Syntax

ssh client ipv6 source { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }

undo ssh client ipv6 source

View

System view

Default Level

3: Manage level

Parameters

ipv6 *ipv6-address*: Specifies a source IPv6 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description

Use the **ssh client ipv6 source** command to specify the source IPv6 address or source interface for the SSH client.

Use the **undo ssh client ipv6 source** command to remove the configuration.

By default, the client uses the source address specified by the route of the device to access the SSH server.

Related commands: **display ssh client source**.

Examples

Specify the source IPv6 address as 2:2::2:2 for the SSH client.

```
<Sysname> system-view
[Sysname] ssh client ipv6 source ipv6 2:2::2:2
```

ssh client source

Syntax

ssh client source { **ip** *ip-address* | **interface** *interface-type interface-number* }

undo ssh client source

View

System view

Default Level

3: Manage level

Parameters

ip *ip-address*: Specifies a source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description

Use the **ssh client source** command to specify the source IPv4 address or source interface of the SSH client.

Use the **undo ssh client source** command to remove the configuration.

By default, an SSH client uses the IP address of the interface specified by the route to access the SSH server.

Related commands: **display ssh client source**.

Examples

Specify the source IPv4 address of the SSH client as 192.168.0.1.

```
<Sysname> system-view
[Sysname] ssh client source ip 192.168.0.1
```

ssh2

Syntax

ssh2 *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View

User view

Default Level

0: Visit level

Parameters

server: IPv4 address or host name of the server, a case-insensitive string of 1 to 20 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **aes128**: Encryption algorithm aes128-cbc
- **des**: Encryption algorithm des-cbc.

prefer-ctos-hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

prefer-kex: Preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

Description

Use the **ssh2** command to establish a connection to an IPv4 SSH server and specify the public key algorithm, the preferred key exchange algorithm, and the preferred encryption algorithms and preferred HMAC algorithms between the client and server.

Note that when the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the encryption algorithm is DSA.

Examples

Log in to remote SSH2.0 server 10.214.50.51, using the following algorithms:

- Preferred key exchange algorithm: DH-group1
- Preferred encryption algorithm from server to client: AES128
- Preferred HMAC algorithm from client to server: MD5
- Preferred HMAC algorithm from server to client: SHA1-96.

```
<Sysname> ssh2 10.214.50.51 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac
md5 prefer-stoc-hmac sha1-96
```

ssh2 ipv6

Syntax

ssh2 ipv6 *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View

User view

Default Level

0: Visit level

Parameters

server: IPv6 address or host name of the server, a case-insensitive string of 1 to 46 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **aes128**: Encryption algorithm aes128-cbc.
- **des**: Encryption algorithm des-cbc.

prefer-ctos-hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

prefer-kex: Preferred key exchange algorithm, default to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1

prefer-stoc-cipher: Preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

Description

Use the **ssh2 ipv6** command to establish a connection to an IPv6 SSH server and specify public key algorithm, the preferred key exchange algorithm, and the preferred encryption algorithms and preferred HMAC algorithms between the client and server.

Note that when the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the encryption algorithm is DSA.

Examples

Login to remote SSH2.0 server 2000::1, setting the algorithms as follows:

- Preferred key exchange algorithm: DH-group1

- Preferred encryption algorithm from server to client: AES128
- Preferred HMAC algorithm from client to server: MD5
- Preferred HMAC algorithm from server to client: SHA1-96.

```
<Sysname> ssh2 ipv6 2000::1 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac
md5 prefer-stoc-hmac sha1-96
```

SFTP Server Configuration Commands

sftp server enable

Syntax

sftp server enable

undo sftp server enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **sftp server enable** command to enable SFTP server.

Use the **undo sftp server enable** command to disable SFTP server.

By default, SFTP server is disabled.

Related commands: **display ssh server**.

Examples

Enable SFTP server.

```
<Sysname> system-view
[Sysname] sftp server enable
```

sftp server idle-timeout

Syntax

sftp server idle-timeout *time-out-value*

undo sftp server idle-timeout

View

System view

Default Level

2: System level

Parameters

time-out-value: Timeout period in minutes. It ranges from 1 to 35,791.

Description

Use the **sftp server idle-timeout** command to set the idle timeout period for SFTP user connections.

Use the **undo sftp server idle-timeout** command to restore the default.

By default, the idle timeout period is 10 minutes.

Related commands: **display ssh server**.

Examples

Set the idle timeout period for SFTP user connections to 500 minutes.

```
<Sysname> system-view
[Sysname] sftp server idle-timeout 500
```

SFTP Client Configuration Commands

bye

Syntax

bye

View

SFTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **bye** command to terminate the connection with a remote SFTP server and return to user view.

This command functions as the **exit** and **quit** commands.

Examples

Terminate the connection with the remote SFTP server.

```
sftp-client> bye
Bye
<Sysname>
```

cd

Syntax

cd [*remote-path*]

View

SFTP client view

Default Level

3: Manage level

Parameters

remote-path: Name of a path on the server.

Description

Use the **cd** command to change the working path on a remote SFTP server. With the argument not specified, the command displays the current working path.

Note

- You can use the **cd ..** command to return to the upper-level directory.
- You can use the **cd /** command to return to the root directory of the system.

Examples

Change the working path to **new1**.

```
sftp-client> cd new1
Current Directory is:
/new1
```

cdup

Syntax

cdup

View

SFTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **cdup** command to return to the upper-level directory.

Examples

From the current working directory /new1, return to the upper-level directory.

```
sftp-client> cdup
```

```
Current Directory is:
/
```

delete

Syntax

delete *remote-file*&<1-10>

View

SFTP client view

Default Level

3: Manage level

Parameters

remote-file&<1-10>: Name of a file on the server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.

Description

Use the **delete** command to delete the specified file(s) from a server.

This command functions as the **remove** command.

Examples

Delete file temp.c from the server.

```
sftp-client> delete temp.c
The following files will be deleted:
/temp.c
Are you sure to delete it? [Y/N]:y
This operation may take a long time. Please wait...

File successfully Removed
```

dir

Syntax

dir [**-a** | **-l**] [*remote-path*]

View

SFTP client view

Default Level

3: Manage level

Parameters

-a: Displays the filenames or the folder names of the specified directory.

-l: Displays in a list form detailed information of the files and folders of the specified directory.

remote-path: Name of the directory to be queried.

Description

Use the **dir** command to display file and folder information under a specified directory.

With the **–a** and **–l** keyword not specified, the command displays detailed information of files and folders under the specified directory in a list form.

With the *remote-path* not specified, the command displays the file and folder information of the current working directory.

This command functions as the **ls** command.

Examples

Display in a list form detailed file and folder information under the current working directory.

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup     1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup      225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup      283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup      225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup        0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup        0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup      225 Sep 28 08:30 pub2
```

display sftp client source

Syntax

display sftp client source

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display sftp client source** command to display the source IP address or source interface currently set for the SFTP client.

If neither source IP address nor source interface is specified for the SFTP client, the system will prompt you to specify the source information.

Related commands: **sftp client source**.

Examples

Display the source IP address of the SFTP client.

```
<Sysname> display sftp client source
The source IP address you specified is 192.168.0.1
```

exit

Syntax

exit

View

SFTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **exit** command to terminate the connection with a remote SFTP server and return to user view.

This command functions as the **bye** and **quit** commands.

Examples

Terminate the connection with the remote SFTP server.

```
sftp-client> exit
Bye
<Sysname>
```

get

Syntax

get *remote-file* [*local-file*]

View

SFTP client view

Default Level

3: Manage level

Parameters

remote-file: Name of a file on the remote SFTP server.

local-file: Name for the local file.

Description

Use the **get** command to download a file from a remote SFTP server and save it locally.

If you do not specify the *local-file* argument, the file will be saved locally with the same name as that on the remote SFTP server.

Examples

Download file temp1.c and save it as temp.c locally.

```
sftp-client> get temp1.c temp.c
Remote  file:/temp1.c --->  Local file: temp.c
Downloading file successfully ended
```

help

Syntax

help [**all** | *command-name*]

View

SFTP client view

Default Level

3: Manage level

Parameters

all: Displays a list of all commands.

command-name: Name of a command.

Description

Use the **help** command to display a list of all commands or the help information of an SFTP client command.

With neither the argument nor the keyword specified, the command displays a list of all commands.

Examples

Display the help information of the **get** command.

```
sftp-client> help get
get remote-path [local-path]  Download file.Default local-path is the same
                         as remote-path
```

ls

Syntax

ls [**-a** | **-l**] [*remote-path*]

View

SFTP client view

Default Level

3: Manage level

Parameters

-a: Displays the filenames or the folder names of the specified directory.

-l: Displays in a list form detailed information of the files and folders of the specified directory

remote-path: Name of the directory to be queried.

Description

Use the **ls** command to display file and folder information under a specified directory.

With the **–a** and **–l** keyword not specified, the command displays detailed information of files and folders under the specified directory in a list form.

With the *remote-path* not specified, the command displays the file and folder information of the current working directory.

This command functions as the **dir** command.

Examples

Display in a list form detailed file and folder information under the current working directory.

```
sftp-client> ls
-rwxrwxrwx   1 noone    nogroup     1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup      225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup      283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup      225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup        0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup        0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup      225 Sep 28 08:30 pub2
```

mkdir

Syntax

mkdir *remote-path*

View

SFTP client view

Default Level

3: Manage level

Parameters

remote-path: Name for the directory on a remote SFTP server.

Description

Use the **mkdir** command to create a directory on a remote SFTP server.

Examples

Create a directory named **test** on the remote SFTP server.

```
sftp-client> mkdir test
New directory created
```

put

Syntax

put *local-file* [*remote-file*]

View

SFTP client view

Default Level

3: Manage level

Parameters

local-file: Name of a local file.

remote-file: Name for the file on a remote SFTP server.

Description

Use the **put** command to upload a local file to a remote SFTP server.

If you do not specify the *remote-file* argument, the file will be saved remotely with the same name as the local one.

Examples

Upload local file temp.c to the remote SFTP server and save it as temp1.c.

```
sftp-client> put temp.c temp1.c
Local file:temp.c --->  Remote file: /temp1.c
Uploading file successfully ended
```

pwd

Syntax

pwd

View

SFTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **pwd** command to display the current working directory of a remote SFTP server.

Examples

Display the current working directory of the remote SFTP server.

```
sftp-client> pwd
/
```

quit

Syntax

quit

View

SFTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **quit** command to terminate the connection with a remote SFTP server and return to user view.

This command functions as the **bye** and **exit** commands.

Examples

Terminate the connection with the remote SFTP server.

```
sftp-client> quit
Bye
<Sysname>
```

remove

Syntax

remove *remote-file*&<1-10>

View

SFTP client view

Default Level

3: Manage level

Parameters

remote-file&<1-10>: Name of a file on an SFTP server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.

Description

Use the **remove** command to delete the specified file(s) from a remote server.

This command functions as the **delete** command.

Examples

Delete file temp.c from the server.

```
sftp-client> remove temp.c
The following files will be deleted:
```

```
/temp.c
Are you sure to delete it? [Y/N]:y
This operation may take a long time.Please wait...

File successfully Removed
```

rename

Syntax

rename *oldname newname*

View

SFTP client view

Default Level

3: Manage level

Parameters

oldname: Original file name or directory name.

newname: New file name or directory name.

Description

Use the **rename** command to change the name of a specified file or directory on an SFTP server.

Examples

Change the name of a file on the SFTP server from temp1.c to temp2.c.

```
sftp-client> rename temp1.c temp2.c
File successfully renamed
```

rmdir

Syntax

rmdir *remote-path*&<1-10>

View

SFTP client view

Default Level

3: Manage level

Parameters

remote-path&<1-10>: Name of the directory on the remote SFTP server. &<1-10> means that you can provide up to 10 directory names that are separated by space.

Description

Use the **rmdir** command to delete the specified directories from an SFTP server.

Examples

On the SFTP server, delete directory **temp1** in the current directory.

```
sftp-client> rmdir temp1
Directory successfully removed
```

sftp

Syntax

sftp *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View

User view

Default Level

3: Manage level

Parameters

server: IPv4 address or host name of the server, a case-insensitive string of 1 to 20 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either dsa or rsa. The default is dsa.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **aes128**: Encryption algorithm aes128-cbc.
- **des**: Encryption algorithm des-cbc.

prefer-ctos-hmac: Preferred HMAC algorithm from client to server, defaulted to sha1.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

prefer-kex: Preferred key exchange algorithm, defaulted to dh-group-exchange.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Preferred encryption algorithm from server to client, defaulted to aes128.

prefer-stoc-hmac: Preferred HMAC algorithm from server to client, defaulted to sha1.

Description

Use the **sftp** command to establish a connection to a remote IPv4 SFTP server and enter SFTP client view.

Note that when the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify

an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the encryption algorithm is DSA.

Examples

Connect to SFTP server 10.1.1.2, using the following algorithms:

- Preferred key exchange algorithm: **dh-group1**.
- Preferred encryption algorithm from server to client: **aes128**.
- Preferred HMAC algorithm from client to server: **md5**.
- Preferred HMAC algorithm from server to client: **sha1-96**.

```
<Sysname> sftp 10.1.1.2 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac md5
prefer-stoc-hmac sha1-96
Input Username:
```

sftp client ipv6 source

Syntax

sftp client ipv6 source { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }

undo sftp client ipv6 source

View

System view

Default Level

3: Manage level

Parameters

ipv6 *ipv6-address*: Specifies a source IPv6 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description

Use the **sftp client ipv6 source** command to specify the source IPv6 address or source interface for an SFTP client.

Use the **undo sftp client ipv6 source** command to remove the configuration.

By default, the client uses the interface address specified by the route of the device to access the SFTP server.

Related commands: **display sftp client source**.

Examples

Specify the source IPv6 address of the SFTP client as 2:2::2:2.

```
<Sysname> system-view
[Sysname] sftp client ipv6 source ipv6 2:2::2:2
```

sftp client source

Syntax

sftp client source { **ip** *ip-address* | **interface** *interface-type interface-number* }

undo sftp client source

View

System view

Default Level

3: Manage level

Parameters

ip *ip-address*: Specifies a source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description

Use the **sftp client source** command to specify the source IPv4 address or interface of an SFTP client.

Use the **undo sftp source-interface** command to remove the configuration.

By default, a client uses the IP address of the interface specified by the route to access the SFTP server.

Related commands: **display sftp client source**.

Examples

Specify the source IP address of the SFTP client as 192.168.0.1.

```
<Sysname> system-view
[Sysname] sftp client source ip 192.168.0.1
```

sftp ipv6

Syntax

sftp ipv6 *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View

User view

Default Level

3: Manage level

Parameters

server: IPv6 address or host name of the server, a case-insensitive string of 1 to 46 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **aes128**: Encryption algorithm aes128-cbc.

- **des**: Encryption algorithm des-cbc.

prefer-ctos-hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

prefer-kex: Preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

Description

Use the **sftp ipv6** command to establish a connection to a remote IPv6 SFTP server and enter SFTP client view.

Note that when the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key. By default, the encryption algorithm is DSA.

Examples

Connect to server 2:5::8:9, using the following algorithms:

- Preferred key exchange algorithm: **dh-group1**.
- Preferred encryption algorithm from server to client: **aes128**.
- Preferred HMAC algorithm from client to server: **md5**.
- Preferred HMAC algorithm from server to client: **sha1-96**.

```
<Sysname> sftp ipv6 2:5::8:9 prefer-kex dh-group1 prefer-stoc-cipher aes128 prefer-ctos-hmac
md5 prefer-stoc-hmac sha1-96
Input Username:
```

11 PKI Configuration Commands

PKI Configuration Commands

attribute

Syntax

attribute *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ**} *attribute-value*

undo attribute { *id* | all }

View

Certificate attribute group view

Default Level

2: System level

Parameters

id: Sequence number of the certificate attribute rule, in the range 1 to 16.

alt-subject-name: Specifies the name of the alternative certificate subject.

fqdn: Specifies the FQDN of the entity.

ip: Specifies the IP address of the entity.

issuer-name: Specifies the name of the certificate issuer.

subject-name: Specifies the name of the certificate subject.

dn: Specifies the distinguished name of the entity.

ctn: Specifies the contain operation.

equ: Specifies the equal operation.

nctn: Specifies the not-contain operation.

nequ: Specifies the not-equal operation.

attribute-value: Value of the certificate attribute, a case-insensitive string of 1 to 128 characters.

all: Specifies all certificate attributes.

Description

Use the **attribute** command to configure the attribute rules of the certificate issuer name, certificate subject name and alternative certificate subject name.

Use the **undo attribute** command to delete the attribute rules of one or all certificates.

By default, there is no restriction on the issuer name, subject name, and alternative subject name of a certificate.

Note that the attribute of the alternative certificate subject name does not appear as a distinguished name, and therefore the **dn** keyword is not available for the attribute.

Examples

Create a certificate attribute rule, specifying that the DN in the subject name includes the string of abc.

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc
```

Create a certificate attribute rule, specifying that the FQDN in the issuer name cannot be the string of abc.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc
```

Create a certificate attribute rule, specifying that the IP address in the alternative subject name cannot be 10.0.0.1.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1
```

ca identifier

Syntax

ca identifier *name*

undo ca identifier

View

PKI domain view

Default Level

2: System level

Parameters

name: Identifier of the trusted CA, a case-insensitive string of 1 to 63 characters.

Description

Use the **ca identifier** command to specify the trusted CA and bind the device with the CA.

Use the **undo ca identifier** command to remove the configuration.

By default, no trusted CA is specified for a PKI domain.

Certificate request, retrieval, revocation, and query all depend on the trusted CA.

Examples

Specify the trusted CA as **new-ca**.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] ca identifier new-ca
```

certificate request entity

Syntax

certificate request entity *entity-name*

undo certificate request entity

View

PKI domain view

Default Level

2: System level

Parameters

entity-name: Name of the entity for certificate request, a case-insensitive string of 1 to 15 characters.

Description

Use the **certificate request entity** command to specify the entity for certificate request.

Use the **undo certificate request entity** command to remove the configuration.

By default, no entity is specified for a PKI domain.

Related commands: **pki entity**.

Examples

Specify the entity for certificate request as **entity1**.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request entity entity1
```

certificate request from

Syntax

certificate request from { **ca** | **ra** }

undo certificate request from

View

PKI domain view

Default Level

2: System level

Parameters

ca: Indicates that the entity requests a certificate from a CA.

ra: Indicates that the entity requests a certificate from an RA.

Description

Use the **certificate request from** command to specify the authority for certificate request.

Use the **undo certificate request from** command to remove the configuration.

By default, no authority is specified for a PKI domain view.

Examples

Specify that the entity requests a certificate from the CA.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request from ca
```

certificate request mode

Syntax

certificate request mode { **auto** [**key-length** *key-length* | **password** { **cipher** | **simple** } *password*]* | **manual** }

undo certificate request mode

View

PKI domain view

Default Level

2: System level

Parameters

auto: Specifies to request a certificate in auto mode.

key-length: Length of the RSA keys, in the range 512 to 2,048 bits. It is 1,024 bits by default.

password: Password for certificate revocation, a case-sensitive string of 1 to 31 characters.

cipher: Specifies to display the password in cipher text.

simple: Specifies to display the password in clear text.

manual: Specifies to request a certificate in manual mode.

Description

Use the **certificate request mode** command to set the certificate request mode.

Use the **undo certificate request mode** command to restore the default.

By default, manual mode is used.

In auto mode, an entity automatically requests a certificate from an RA or CA when it has no certificate or when the existing certificate is about to expire. In manual mode, all operations associated with certificate request are carried out manually.

Related commands: **pki request-certificate**.

Examples

Specify to request a certificate in auto mode.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request mode auto
```

certificate request polling

Syntax

certificate request polling { **count** *count* | **interval** *minutes* }

undo certificate request polling { **count** | **interval** }

View

PKI domain view

Default Level

2: System level

Parameters

count: Maximum number of attempts to poll the status of the certificate request, in the range 1 to 100.

minutes: Polling interval, in the range 5 to 168 minutes.

Description

Use the **certificate request polling** command to specify the certificate request polling interval and attempt limit.

Use the **undo certificate request polling** command to restore the defaults.

By default, the polling is executed every 20 minutes for up to 50 times.

After an applicant makes a certificate request, the CA may need a long period of time if it verifies the certificate request manually. During this period, the applicant needs to query the status of the request periodically to get the certificate as soon as possible after the certificate is signed.

Related commands: **display pki certificate**.

Examples

Specify the polling interval as 15 minutes and the maximum number of attempts as 40.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request polling interval 15
[Sysname-pki-domain-1] certificate request polling count 40
```

certificate request url

Syntax

certificate request url *url-string*

undo certificate request url

View

PKI domain view

Default Level

2: System level

Parameters

url-string: URL of the server for certificate request, a case-insensitive string of 1 to 127 characters. It comprises the location of the server and the location of CGI command interface script in the format of *http: //server_location/ca_script_location*, where *server_location* must be an IP address and does not support domain name resolution currently.

Description

Use the **certificate request url** command to specify the URL of the server for certificate request through SCEP.

Use the **undo certificate request url** command to remove the configuration.

By default, no URL is specified for a PKI domain.

Examples

Specify the URL of the server for certificate request.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request url
http://169.254.0.100/certsrv/mscep/mscep.dll
```

common-name

Syntax

common-name *name*

undo common-name

View

PKI entity view

Default Level

2: System level

Parameters

name: Common name of an entity, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use the **common-name** command to configure the common name of an entity, which can be, for example, the user name.

Use the **undo common-name** command to remove the configuration.

By default, no common name is specified.

Examples

Configure the common name of an entity as **test**.

```
<Sysname> system-view
[Sysname] pki entity 1
```

```
[Sysname-pki-entity-1] common-name test
```

country

Syntax

country *country-code-str*

undo country

View

PKI entity view

Default Level

2: System level

Parameters

country-code-str: Country code for the entity, a 2-character case-insensitive string.

Description

Use the **country** command to specify the code of the country to which an entity belongs. It is a standard 2-character code, for example, CN for China.

Use the **undo country** command to remove the configuration.

By default, no country code is specified.

Examples

Set the country code of an entity to **CN**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] country CN
```

crl check

Syntax

crl check { **disable** | **enable** }

View

PKI domain view

Default Level

2: System level

Parameters

disable: Disables CRL checking.

enable: Enables CRL checking.

Description

Use the **crl check** command to enable or disable CRL checking.

By default, CRL checking is enabled.

CRLs are files issued by the CA to publish all certificates that have been revoked. Revocation of a certificate may occur before the certificate expires. CRL checking is intended for checking whether a certificate has been revoked. A revoked certificate is no longer trusted.

Examples

Disable CRL checking.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl check disable
```

crl update-period

Syntax

crl update-period *hours*

undo crl update-period

View

PKI domain view

Default Level

2: System level

Parameters

hours: CRL update period, in the range 1 to 720 hours.

Description

Use the **crl update-period** command to set the CRL update period, that is, the interval at which the PKI entity downloads the latest CRLs.

Use the **undo crl update-period** command to restore the default.

By default, the CRL update period depends on the next update field in the CRL file.

The CRL update period is the interval at which a PKI entity with a certificate downloads a CRL from LDAP server.

Examples

Set the CRL update period to 20 hours.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl update-period 20
```

crl url

Syntax

crl url *url-string*

undo crl url

View

PKI domain view

Default Level

2: System level

Parameters

url-string: URL of the CRL distribution point, a case-insensitive string of 1 to 127 characters in the format of *ldap://server_location* or http://*server_location,* where *server_location* must be an IP address and does not support domain name resolution currently.

Description

Use the **crl url** command to specify the URL of the CRL distribution point.

Use the **undo crl url** command to remove the configuration.

By default, no CRL distribution point URL is specified.

Note that when the URL of the CRL distribution point is not set, you should acquire the CA certificate and a local certificate, and then acquire a CRL through SCEP.

Examples

Specify the URL of the CRL distribution point.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl url ldap://169.254.0.30
```

display pki certificate

Syntax

display pki certificate { { **ca** | **local** } **domain** *domain-name* | **request-status** }

View

Any view

Default Level

2: System level

Parameters

ca: Displays the CA certificate.

local: Displays the local certificate.

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

request-status: Displays the status of a certificate request.

Description

Use the **display pki certificate** command to display the contents or request status of a certificate.

Related commands: **pki retrieval-certificate**, **pki domain** and **certificate request polling**.

Examples

Display the local certificate.

```
<Sysname> display pki certificate local domain 1
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number:
         10B7D4E3 00010000 0086
      Signature Algorithm: md5WithRSAEncryption
      Issuer:
         emailAddress=myca@aabbcc.net
         C=CN
         ST=Country A
         L=City X
         O=abc
         OU=bjs
         CN=new-ca
      Validity
         Not Before: Jan 13 08:57:21 2004 GMT
         Not After : Jan 20 09:07:21 2005 GMT
      Subject:
         C=CN
         ST=Country B
         L=City Y
         CN=pki test
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (512 bit)
            Modulus (512 bit):
               00D41D1F …
            Exponent: 65537 (0x10001)
      X509v3 extensions:
         X509v3 Subject Alternative Name:
         DNS: hyf.xxyyzz.net
         X509v3 CRL Distribution Points:
         URI:http://1.1.1.1:447/myca.crl
         …         …
   Signature Algorithm: md5WithRSAEncryption
      A3A5A447 4D08387D …
```

Table 11-1 display pki certificate command output description

Field	Description
Version	Version of the certificate
Serial Number	Serial number of the certificate
Signature Algorithm	Signature algorithm
Issuer	Issuer of the certificate

Field	Description
Validity	Validity period of the certificate
Subject	Entity holding the certificate
Subject Public Key Info	Public key information of the entity
X509v3 extensions	Extensions of the X.509 (version 3) certificate
X509v3 CRL Distribution Points	Distribution points of X.509 (version 3) CRLs

display pki certificate access-control-policy

Syntax

display pki certificate access-control-policy { *policy-name* | **all** }

View

Any view

Default Level

1: Monitor level

Parameters

policy-name: Name of the certificate attribute-based access control policy, a string of 1 to 16 characters.

all: Specifies all certificate attribute-based access control policies.

Description

Use the **display pki certificate access-control-policy** command to display information about a specified or all certificate attribute-based access control policies.

Examples

Display information about the certificate attribute-based access control policy named mypolicy.

```
<Sysname> display pki certificate access-control-policy mypolicy
 access-control-policy name: mypolicy
    rule  1 deny    mygroup1
    rule  2 permit  mygroup2
```

Table 11-2 display pki certificate access-control-policy command output description

Field	Description
access-control-policy	Name of the certificate attribute-based access control policy
rule number	Number of the access control rule

display pki certificate attribute-group

Syntax

display pki certificate attribute-group { *group-name* | **all** }

View

Any view

Default Level

1: Monitor level

Parameters

group-name: Name of a certificate attribute group, a string of 1 to 16 characters.

all: Specifies all certificate attribute groups.

Description

Use the **display pki certificate attribute-group** command to display information about a specified or all certificate attribute groups.

Examples

Display information about certificate attribute group mygroup.

```
<Sysname> display pki certificate attribute-group mygroup
 attribute group name: mygroup
     attribute  1 subject-name    dn   ctn   abc
     attribute  2 issuer-name     fqdn  nctn  app
```

Table 11-3 display pki certificate attribute-group command output description

Field	Description
attribute group name	Name of the certificate attribute group
attribute *number*	Number of the attribute rule
subject-name	Name of the certificate subject
dn	DN of the entity
ctn	Indicates the contain operations
abc	Value of attribute 1
issuer-name	Name of the certificate issuer
fqdn	FQDN of the entity
nctn	Indicates the not-contain operations
app	Value of attribute 2

display pki crl domain

Syntax

display pki crl domain *domain-name*

View

Any view

Default Level

2: System level

Parameters

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

Description

Use the **display pki crl domain** command to display the locally saved CRLs.

Related commands: **pki retrieval-crl**, **pki domain**.

Examples

Display the locally saved CRLs.

```
<Sysname> display pki crl domain 1
 Certificate Revocation List (CRL):
      Version 2 (0x1)
      Signature Algorithm: sha1WithRSAEncryption
      Issuer:
         C=CN
         O=abc
         OU=soft
         CN=A Test Root
      Last Update: Jan  5 08:44:19 2004 GMT
      Next Update: Jan  5 21:42:13 2004 GMT
      CRL extensions:
         X509v3 Authority Key Identifier:
         keyid:0F71448E E075CAB8 ADDB3A12 0B747387 45D612EC
         Revoked Certificates:
         Serial Number: 05a234448E…
         Revocation Date: Sep 6 12:33:22 2004 GMT
         CRL entry extensions:…
         Serial Number: 05a278445E…
         Revocation Date: Sep 7 12:33:22 2004 GMT
         CRL entry extensions:…
```

Table 11-4 display pki crl domain command output description

Field	Description
Version	Version of the CRLs
Signature Algorithm	Signature algorithm used by the CRLs
Issuer	CA issuing the CRLs
Last Update	Last update time
Next Update	Next update time
CRL extensions	Extensions of CRL

Field	Description
X509v3 Authority Key Identifier	CA issuing the CRLs. The certificate version is X.509v3.
keyid	ID of the public key A CA may have multiple key pairs. This field indicates the key pair used by the CRL's signature.
Revoked Certificates	Revoked certificates
Serial Number	Serial number of the revoked certificate
Revocation Date	Revocation date of the certificate

fqdn

Syntax

fqdn *name-str*

undo fqdn

View

PKI entity view

Default Level

2: System level

Parameters

name-str: Fully qualified domain name (FQDN) of an entity, a case-insensitive string of 1 to 127 characters.

Description

Use the **fqdn** command to configure the FQDN of an entity.

Use the **undo fqdn** command to remove the configuration.

By default, no FQDN is specified for an entity.

An FQDN is the unique identifier of an entity on a network. It consists of a host name and a domain name and can be resolved into an IP address.

Examples

Configure the FQDN of an entity as **pki.domain-name.com**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] fqdn pki.domain-name.com
```

ip (PKI entity view)

Syntax

ip *ip-address*

undo ip

View

PKI entity view

Default Level

2: System level

Parameters

ip-address: IP address for an entity.

Description

Use the **ip** command to configure the IP address of an entity.

Use the **undo ip** command to remove the configuration.

By default, no IP address is specified for an entity.

Examples

Configure the IP address of an entity as 11.0.0.1.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] ip 11.0.0.1
```

ldap-server

Syntax

ldap-server ip *ip-address* [**port** *port-number*] [**version** *version-number*]

undo ldap-server

View

PKI domain view

Default Level

2: System level

Parameters

ip-address: IP address of the LDAP server, in dotted decimal format.

port-number: Port number of the LDAP server, in the range 1 to 65535. The default is 389.

version-number: LDAP version number, either 2 or 3. By default, it is 2.

Description

Use the **ldap-server** command to specify an LDAP server for a PKI domain.

Use the **undo ldap-server** command to remove the configuration.

By default, no LDP server is specified for a PKI domain.

Examples

Specify an LDAP server for PKI domain 1.

```
<Sysname> system-view
```

```
[Sysname] pki domain 1
[Sysname-pki-domain-1] ldap-server ip 169.254.0.30
```

locality

Syntax

locality *locality-name*

undo locality

View

PKI entity view

Default Level

2: System level

Parameters

locality-name: Name for the geographical locality, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use the **locality** command to configure the geographical locality of an entity, which can be, for example, a city name.

Use the **undo locality** command to remove the configuration.

By default, no geographical locality is specified for an entity.

Examples

Configure the locality of an entity as **city**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] locality city
```

organization

Syntax

organization *org-name*

undo organization

View

PKI entity view

Default Level

2: System level

Parameters

org-name: Organization name, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use the **organization** command to configure the name of the organization to which the entity belongs.

Use the **undo organization** command to remove the configuration.

By default, no organization name is specified for an entity.

Examples

Configure the name of the organization to which an entity belongs as **org-name**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] organization org-name
```

organization-unit

Syntax

organization-unit *org-unit-name*

undo organization-unit

View

PKI entity view

Default Level

2: System level

Parameters

org-unit-name: Organization unit name for distinguishing different units in an organization, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use the **organization-unit** command to specify the name of the organization unit to which this entity belongs.

Use the **undo organization-unit** command to remove the configuration.

By default, no organization unit name is specified for an entity.

Examples

Configure the name of the organization unit to which an entity belongs as **unit-name**.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] organization-unit unit-name
```

pki certificate access-control-policy

Syntax

pki certificate access-control-policy *policy-name*

undo pki certificate access-control-policy { *policy-name* | **all** }

View

System view

Default Level

2: System level

Parameters

policy-name: Name of the certificate attribute-based access control policy, a case-insensitive string of 1 to 16 characters. It cannot be “a”, “al” or “all”.

all: Specifies all certificate attribute-based access control policies.

Description

Use the **pki certificate access-control-policy** command to create a certificate attribute-based access control policy and enter its view.

Use the **undo pki certificate access-control-policy** command to remove a specified or all certificate attribute-based access control policies.

No access control policy exists by default.

Examples

Configure an access control policy named **mypolicy** and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy]
```

pki certificate attribute-group

Syntax

pki certificate attribute-group *group-name*

undo pki certificate attribute-group { *group-name* | **all** }

View

System view

Default Level

2: System level

Parameters

group-name: Name for the certificate attribute group, a case-insensitive string of 1 to 16 characters. It cannot be “a”, “al” or “all”.

all: Specifies all certificate attribute groups.

Description

Use the **pki certificate attribute-group** command to create a certificate attribute group and enter its view.

Use the **undo pki certificate attribute-group** command to delete one or all certificate attribute groups.

By default, no certificate attribute group exists.

Examples

Create a certificate attribute group named **mygroup** and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup]
```

pki delete-certificate

Syntax

pki delete-certificate { **ca** | **local** } **domain** *domain-name*

View

System view

Default Level

2: System level

Parameters

ca: Deletes the locally stored CA certificate.

local: Deletes the locally stored local certificate.

domain-name: Name of the PKI domain whose certificates are to be deleted, a string of 1 to 15 characters.

Description

Use the **pki delete-certificate** command to delete the certificate locally stored for a PKI domain.

Examples

Delete the local certificate for PKI domain cer.

```
<Sysname> system-view
[Sysname] pki delete-certificate local domain cer
```

pki domain

Syntax

pki domain *domain-name*

undo pki domain *domain-name*

View

System view

Default Level

2: System level

Parameters

domain-name: PKI domain name, a case-insensitive string of 1 to 15 characters.

Description

Use the **pki domain** command to create a PKI domain and enter PKI domain view or enter the view of an existing PKI domain.

Use the **undo pki domain** command to remove a PKI domain.

By default, no PKI domain exists.

Examples

Create a PKI domain and enter its view.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1]
```

pki entity

Syntax

pki entity *entity-name*

undo pki entity *entity-name*

View

System view

Default Level

2: System level

Parameters

entity-name: Name for the entity, a case-insensitive string of 1 to 15 characters.

Description

Use the **pki entity** command to create a PKI entity and enter PKI entity view.

Use the **undo pki entity** command to remove a PKI entity.

By default, no entity exists.

You can configure a variety of attributes for an entity in PKI entity view. An entity is intended only for convenience of reference by other commands.

Examples

Create a PKI entity named **en** and enter its view.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en]
```

pki import-certificate

Syntax

pki import-certificate { **ca** | **local** } **domain** *domain-name* { **der** | **p12** | **pem** } [**filename** *filename*]

View

System view

Default Level

2: System level

Parameters

ca: Specifies the CA certificate.

local: Specifies the local certificate.

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

der: Specifies the certificate format of DER.

p12: Specifies the certificate format of P12.

pem: Specifies the certificate format of PEM.

filename: Name of the certificate file, a case-insensitive string of 1 to 127 characters. It defaults to *domain-name*_ca.cer, *domain-name*_local.cer, or *domain-name*_peerentity_*entity-name*.cer, the name for the file to be created to save the imported certificate.

Description

Use the **pki import-certificate** command to import a CA certificate or local certificate from a file and save it locally.

Related commands: **pki domain**.

Examples

Import the CA certificate for PKI domain cer in the format of PEM.

```
<Sysname> system-view
[Sysname] pki import-certificate ca domain cer pem
```

pki request-certificate domain

Syntax

pki request-certificate domain *domain-name* [*password*] [**pkcs10** [**filename** *filename*]]

View

System view

Default Level

2: System level

Parameters

domain-name: Name of the PKI domain name, a string of 1 to 15 characters.

password: Password for certificate revocation, a case-sensitive string of 1 to 31 characters.

pkcs10: Displays the BASE64-encoded PKCS#10 certificate request.

filename: Name of the file for saving the PKCS#10 certificate request, a case-insensitive string of 1 to 127 characters.

Description

Use the **pki request-certificate domain** command to request a local certificate from a CA through SCEP. If SCEP fails, you can use the **pkcs10** keyword to save the local certificate request in BASE64 format and send it to the CA by an out-of-band means like phone, disk or e-mail.

This operation will not be saved in the configuration file.

Related commands: **pki domain**.

Examples

Display the PKCS#10 certificate request information.

```
<Sysname> system-view
[Sysname] pki request-certificate domain 1 pkcs10
[Sysname] pki request-certificate domain 1 pkcs10
-----BEGIN CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqajCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAw5Drj8ofs9THA4ezkDcQPBy8pvH1kumampPsJmx8sGG52NFtbrDTnTT5
ALx3LJijB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3ol2z7Nvdu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYyl1WCtkLkECAwEAAaAAMA0G
CSqGSIb3DQEBBAUAA4GBAA8E7BaIdmT6NVCZgv/I/1tqZH3TS4e4H9Qo5NiCKiEw
R8owVmA0XVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mn1ro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsa1lQOHS7YMvnop6hXAQlkM4c
-----END CERTIFICATE REQUEST-----
```

pki retrieval-certificate

Syntax

pki retrieval-certificate { **ca** | **local** } **domain** *domain-name*

View

System view

Default Level

2: System level

Parameters

ca: Retrieves the CA certificate.

local: Retrieves the local certificate.

domain-name: Name of the PKI domain used for certificate request.

Description

Use the **pki retrieval-certificate** command to retrieve a certificate from the server for certificate distribution.

Related commands: **pki domain**.

Examples

Retrieve the CA certificate from the certificate issuing server.

```
<Sysname> system-view
[Sysname] pki retrieval-certificate ca domain 1
```

pki retrieval-crl domain

Syntax

pki retrieval-crl domain *domain-name*

View

System view

Default Level

2: System level

Parameters

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

Description

Use the **pki retrieval-crl domain** command to retrieve the latest CRLs from the server for CRL distribution.

CRLs are used to verify the validity of certificates.

Related commands: **pki domain**.

Examples

Retrieve CRLs.

```
<Sysname> system-view
[Sysname] pki retrieval-crl domain 1
```

pki validate-certificate

Syntax

pki validate-certificate { **ca** | **local** } **domain** *domain-name*

View

System view

Default Level

2: System level

Parameters

ca: Verifies the CA certificate.

local: Verifies the local certificate.

domain-name: Name of the PKI domain to which the certificate to be verified belongs, a string of 1 to 15 characters.

Description

Use the **pki validate-certificate** command to verify the validity of a certificate.

The focus of certificate validity verification is to check that the certificate is signed by the CA and that the certificate has neither expired nor been revoked.

Related commands: **pki domain**.

Examples

Verify the validity of the local certificate.

```
<Sysname> system-view
[Sysname] pki validate-certificate local domain 1
```

root-certificate fingerprint

Syntax

root-certificate fingerprint { **md5** | **sha1** } *string*

undo root-certificate fingerprint

View

PKI domain view

Default Level

2: System level

Parameters

md5: Uses an MD5 fingerprint.

sha1: Uses a SHA1 fingerprint.

string: Fingerprint to be used. An MD5 fingerprint must be a string of 32 characters in hexadecimal. A SHA1 fingerprint must be a string of 40 characters in hexadecimal.

Description

Use the **root-certificate fingerprint** command to configure the fingerprint to be used for verifying the validity of the CA root certificate.

Use the **undo root-certificate fingerprint** command to remove the configuration.

By default, no fingerprint is configured for verifying the validity of the CA root certificate.

Examples

Configure an MD5 fingerprint for verifying the validity of the CA root certificate.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] root-certificate fingerprint md5 12EF53FA355CD23E12EF53FA355CD23E
```

Configure a SHA1 fingerprint for verifying the validity of the CA root certificate.

```
[Sysname-pki-domain-1]           root-certificate           fingerprint           sha1
D1526110AAD7527FB093ED7FC037B0B3CDDDAD93
```

rule (access control policy view)

Syntax

rule [*id*] { **deny** | **permit** } *group-name*

undo rule { *id* | **all** }

View

Access control policy view

Default Level

2: System level

Parameters

id: Number of the certificate attribute access control rule, in the range 1 to 16. The default is the smallest unused number in this range.

deny: Indicates that a certificate whose attributes match an attribute rule in the specified attribute group is considered invalid and denied.

permit: Indicates that a certificate whose attributes match an attribute rule in the specified attribute group is considered valid and permitted.

group-name: Name of the certificate attribute group to be associated with the rule, a case-insensitive string of 1 to 16 characters. It cannot be “a”, “al” or “all”.

all: Specifies all access control rules.

Description

Use the **rule** command to create a certificate attribute access control rule.

Use the **undo rule** command to delete a specified or all access control rules.

By default, no access control rule exists.

Note that a certificate attribute group must exist to be associated with a rule.

Examples

Create an access control rule, specifying that a certificate is considered valid when it matches an attribute rule in certificate attribute group mygroup.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy] rule 1 permit mygroup
```

state

Syntax

state *state-name*

undo state

View

PKI entity view

Default Level

2: System level

Parameters

state-name: State or province name, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description

Use the **state** command to specify the name of the state or province where an entity resides.

Use the **undo state** command to remove the configuration.

By default, no state or province is specified.

Examples

Specify the state where an entity resides.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] state country
```

12 SSL Configuration Commands

SSL Configuration Commands

ciphersuite

Syntax

ciphersuite [**rsa_aes_128_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha**] *

View

SSL server policy view

Default Level

2: System level

Parameters

rsa_aes_128_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit AES_CBC, and the MAC algorithm of SHA.

rsa_des_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of DES_CBC, and the MAC algorithm of SHA.

rsa_rc4_128_md5: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of MD5.

rsa_rc4_128_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of SHA.

Description

Use the **ciphersuite** command to specify the cipher suite(s) for an SSL server policy to support.

By default, an SSL server policy supports all cipher suites.

With no keyword specified, the command configures an SSL server policy to support all cipher suites.

Related commands: **display ssl server-policy**.

Examples

Specify the cipher suites for SSL server policy policy1 to support as **rsa_rc4_128_md5** and **rsa_rc4_128_sha**.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] ciphersuite rsa_rc4_128_md5 rsa_rc4_128_sha
```

client-verify enable

Syntax

client-verify enable

undo client-verify enable

View

SSL server policy view

Default Level

2: System level

Parameters

None

Description

Use the **client-verify enable** command to enable certificate-based SSL client authentication, that is, to enable the SSL server to perform certificate-based authentication of the client during the SSL handshake process.

Use the **undo client-verify enable** command to restore the default.

By default, certificate-based SSL client authentication is disabled.

Examples

Enable certificate-based client authentication.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] client-verify enable
```

close-mode wait

Syntax

close-mode wait

undo close-mode wait

View

SSL server policy view

Default Level

2: System level

Parameters

None

Description

Use the **close-mode wait** command to set the SSL connection close mode to wait. In this mode, after sending a close-notify message to a client, the server does not close the connection until it receives a close-notify message from the client.

Use the **undo close-mode wait** command to restore the default.

By default, an SSL server sends a close-notify alert message to the client and close the connection without waiting for the close-notify alert message from the client.

Related commands: **display ssl server-policy**.

Examples

Set the SSL connection close mode to wait mode.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] close-mode wait
```

display ssl client-policy

Syntax

display ssl client-policy { *policy-name* | **all** }

View

Any view

Default Level

1: Monitor level

Parameters

policy-name: SSL client policy name, a case-insensitive string of 1 to 16 characters.

all: Displays information about all SSL client policies.

Description

Use the **display ssl client-policy** command to view information about a specified or all SSL client policies.

Examples

Display information about SSL client policy policy1.

```
<Sysname> display ssl client-policy policy1
 SSL Client Policy: policy1
    SSL Version: SSL 3.0
    PKI Domain: 1
    Prefer Ciphersuite:
       RSA_RC4_128_SHA
```

Table 12-1 display ssl client-policy command output description

Field	Description
SSL Client Policy	SSL client policy name
SSL Version	Version of the protocol used by the SSL client policy, SSL 3.0 or TLS 1.0.
PKI Domain	PKI domain of the SSL client policy
Prefer Ciphersuite	Preferred cipher suite of the SSL client policy

display ssl server-policy

Syntax

display ssl server-policy { *policy-name* | **all** }

View

Any view

Default Level

1: Monitor level

Parameters

policy-name: SSL server policy name, a case-insensitive string of 1 to 16 characters.

all: Displays information about all SSL server policies.

Description

Use the **display ssl server-policy** command to view information about a specified or all SSL server policies.

Examples

Display information about SSL server policy policy1.

```
<Sysname> display ssl server-policy policy1
 SSL Server Policy: policy1
    PKI Domain: domain1
    Ciphersuite:
       RSA_RC4_128_MD5
       RSA_RC4_128_SHA
       RSA_DES_CBC_SHA
       RSA_AES_128_CBC_SHA
    Handshake Timeout: 3600
    Close-mode: wait disabled
    Session Timeout: 3600
    Session Cachesize: 500
    Client-verify: disabled
```

Table 12-2 display ssl server-policy command output description

Field	Description
SSL Server Policy	SSL server policy name
PKI Domain	PKI domain used by the SSL server policy
Ciphersuite	Cipher suite supported by the SSL server policy
Handshake Timeout	Handshake timeout time of the SSL server policy, in seconds
Close-mode	Close mode of the SSL server policy, which can be: • wait disabled: In this mode, the server sends a close-notify message to the client and then closes the connection immediately without waiting for the close-notify message of the client. • wait enabled: In this mode, the server sends a close-notify message to the client and then waits for the close-notify message of the client. Only after receiving the expected message, does the server close the connection.
Session Timeout	Session timeout time of the SSL server policy, in seconds
Session Cachesize	Maximum number of buffered sessions of the SSL server policy
Client-verify	Whether client authentication is enabled

handshake timeout

Syntax

handshake timeout *time*

undo handshake timeout

View

SSL server policy view

Default Level

2: System level

Parameters

time: Handshake timeout time in seconds, in the range 180 to 7,200.

Description

Use the **handshake timeout** command to set the handshake timeout time for an SSL server policy.

Use the **undo handshake timeout** command to restore the default.

By default, the handshake timeout time is 3,600 seconds.

If the SSL server does not receive any packet from the SSL client before the handshake timeout time expires, the SSL server will terminate the handshake process.

Related commands: **display ssl server-policy**.

Examples

Set the handshake timeout time of SSL server policy policy1 to 3,000 seconds.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] handshake timeout 3000
```

pki-domain

Syntax

pki-domain *domain-name*

undo pki-domain

View

SSL server policy view, SSL client policy view

Default Level

2: System level

Parameters

domain-name: Name of a PKI domain, a case-insensitive string of 1 to 15 characters.

Description

Use the **pki-domain** command to specify a PKI domain for an SSL server policy or SSL client policy.

Use the **undo pki-domain** command to restore the default.

By default, no PKI domain is configured for an SSL server policy or SSL client policy.

Related commands: **display ssl server-policy** and **display ssl client-policy**.

Examples

Configure SSL server policy policy1 to use the PKI domain named server-domain.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] pki-domain server-domain
```

Configure SSL client policy policy1 to use the PKI domain named client-domain.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] pki-domain client-domain
```

prefer-cipher

Syntax

prefer-cipher { **rsa_aes_128_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha** }

undo prefer-cipher

View

SSL client policy view

Default Level

2: System level

Parameters

rsa_aes_128_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit AES_CBC, and the MAC algorithm of SHA.

rsa_des_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of DES_CBC, and the MAC algorithm of SHA.

rsa_rc4_128_md5: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of MD5.

rsa_rc4_128_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of SHA.

Description

Use the **prefer-cipher** command to specify the preferred cipher suite for an SSL client policy.

Use the **undo prefer-cipher** command to restore the default.

By default, the preferred cipher suite for an SSL client policy is **rsa_rc4_128_md5**.

Related commands: **display ssl client-policy**.

Examples

Set the preferred cipher suite for SSL client policy policy1 to **rsa_aes_128_cbc_sha**.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] prefer-cipher rsa_aes_128_cbc_sha
```

session

Syntax

session { **cachesize** *size* | **timeout** *time* } *

undo session { **cachesize** | **timeout** } *

View

SSL server policy view

Default Level

2: System level

Parameters

size: Maximum number of cached sessions, in the range 100 to 1,000.

time: Caching timeout time in seconds, in the range 1,800 to 72,000.

Description

Use the **session** command to set the maximum number of cached sessions and the caching timeout time.

Use the **undo session** command to restore the default.

By default, the maximum number of cached sessions is 500 and the caching timeout time is 3,600 seconds.

The process of the session parameters negotiation and session establishment by using the SSL handshake protocol is quite complicated. SSL allows reusing the negotiated session parameters to establish sessions. Therefore, the SSL server needs to maintain information about existing sessions. Note that the number of sessions and the time that the session information will be maintained are limited:

- If the number of sessions in the cache reaches the maximum, SSL rejects to cache new sessions.
- If a session exists in the cache for a period equal to the caching timeout time, SSL will remove the information of the session.

Related commands: **display ssl server-policy**.

Examples

Set the caching timeout time to 4,000 seconds and the maximum number of cached sessions to 600.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] session timeout 4000 cachesize 600
```

ssl client-policy

Syntax

ssl client-policy *policy-name*

undo ssl client-policy { *policy-name* | **all** }

View

System view

Default Level

2: System level

Parameters

policy-name: SSL client policy name, a case-insensitive string of 1 to 16 characters, which cannot be “a”, “al” and “all”.

all: Specifies all SSL client policies.

Description

Use the **ssl client-policy** command to create an SSL policy and enter its view.

Use the **undo ssl client-policy** command to remove a specified or all SSL client policies.

Related commands: **display ssl client-policy**.

Examples

Create an SSL client policy named policy1 and enter its view.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1]
```

ssl server-policy

Syntax

ssl server-policy *policy-name*

undo ssl server-policy { *policy-name* | **all** }

View

System view

Default Level

2: System level

Parameters

policy-name: SSL server policy name, a case-insensitive string of 1 to 16 characters, which cannot be “a”, “al” and “all”.

all: Specifies all SSL server policies.

Description

Use the **ssl server-policy** command to create an SSL server policy and enter its view.

Use the **undo ssl server-policy** command to remove a specified or all SSL server policies.

Note that you cannot delete an SSL server policy that has been associated with one or more application layer protocols.

Examples

Create an SSL server policy named **policy1** and enter its view.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1]
```

version

Syntax

version { **ssl3.0** | **tls1.0** }

undo version

View

SSL client policy view

Default Level

2: System level

Parameters

ssl3.0: Specifies SSL 3.0.

tls1.0: Specifies TLS 1.0.

Description

Use the **version** command to specify the SSL protocol version for an SSL client policy.

Use the **undo version** command to restore the default.

By default, the SSL protocol version for an SSL client policy is TLS 1.0.

Related commands: **display ssl client-policy**.

Examples

Specify the SSL protocol version for SSL client policy policy1 as SSL 3.0.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] version ssl3.0
```

13 Public Key Configuration Commands

Public Key Configuration Commands

display public-key local public

Syntax

display public-key local { **dsa** | **rsa** } **public**

View

Any view

Default Level

1: Monitor level

Parameters

dsa: DSA key pair.

rsa: RSA key pair.

Description

Use the **display public-key local public** command to display the public key information of the local key pair(s).

Related commands: **public-key local create**.

Examples

Display the public key information of the local RSA key pairs.

```
<Sysname> display public-key local rsa public

=====================================================
Time of Key pair created: 19:59:16  2007/10/25
Key name: HOST_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100BC4C392A97734A633BA0F1DB01F84E
B51228EC86ADE1DBA597E0D9066FDC4F04776CEA3610D2578341F5D049143656F1287502C06D39D39F28F0F5
CBA630DA8CD1C16ECE8A7A65282F2407E8757E7937DCCDB5DB620CD1F471401B7117139702348444A2D89004
97A87B8D5F13D61C4DEFA3D14A7DC07624791FC1D226F62DF3020301
0001
=====================================================
Time of Key pair created: 19:59:17  2007/10/25
Key name: SERVER_KEY
```

```
Key type: RSA Encryption Key
=====================================================
Key code:
307C300D06092A864886F70D0101010500036B003068026100C51AF7CA926962284A4654B2AACC7B2AE12B2B
1EABFAC1CDA97E42C3C10D7A70D1012BF23ADE5AC4E7AAB132CFB6453B27E054BFAA0A85E113FBDE751EE0EC
EF659529E857CF8C211E2A03FD8F10C5BEC162B2989ABB5D299D1E4E27A13C7DD10203010001
```

Display the public key information of the local DSA key pair.

```
<Sysname> display public-key local dsa public

=====================================================
Time of Key pair created: 20:00:16  2007/10/25
Key name: HOST_KEY
Key type: DSA Encryption Key
=====================================================
Key code:
308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD96E5F061C4F0A4
23F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1EDBD13EC8B274DA9F75BA26CCB987
723602787E922BA84421F22C3C89CB9B06FD60FE01941DDD77FE6B12893DA76EEBC1D128D97F0678D7722B53
41C8506F358214B16A2FAC4B368950387811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F
0281810082269009E14EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B
20CD35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B612391C76C1FB2
E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC9B09EEF
038185000281810CCF1F78E0860BE937FD3CA07D2F2A1B66E74E5D1E16693EB374D677A7A6124EBABD59FE4
8796C56F3FF919F999AEB97D1F2B83D9B98AC09BC1F72E80DBE337CB29989A23378EB21C38EE083F11ED6DC8
D4DBE001BA85450CEA071C2A471C83761E4CF32C174B418612CDD597B441F0CAA05DC01CB93A0ABB247C06FB
A4C79054
```

display public-key peer

Syntax

display public-key peer [**brief** | **name** *publickey-name*]

View

Any view

Default Level

1: Monitor level

Parameters

brief: Displays brief information about all the public keys of peers.

name *publickey-name*: Specifies a peer's host public key by its name, which is a case-sensitive string of 1 to 64 characters.

Description

Use the **display public-key peer** command to display information about the specified or all locally saved public keys of peers.

With neither the **brief** keyword nor the **name** *publickey-name* combination specified, the command displays detailed information about all locally saved public keys of peers.

You can use the **public-key peer** command or the **public-key peer import sshkey** command to get a local copy of the public keys of a peer.

Related commands: **public-key peer**, **public-key peer import sshkey**.

Examples

Display detailed information about the peer host public key named **idrsa**.

```
<Sysname> display public-key peer name idrsa
=====================================
  Key Name  : idrsa
  Key Type  : RSA
  Key Module: 1024
=====================================
Key Code:
30819D300D06092A864886F70D010101050003818B003081870281810 09C46A8710216CEC0C01C7CE136BA76
C79AA6040E79F9E305E453998C7ADE8276069410803D5974F708496947AB39B3F39C5CE56C95B6AB7442D563
93BF241F99A639DD02D9E29B1F5C1FD05CC1C44FBD6CFFB58BE6F035FAA2C596B27D1231D159846B7CB9A775
7C5800FADA9FD72F65672F4A549EE99F63095E11BD37789955020123
```

Display brief information about all locally saved public keys of the peers.

```
<Sysname> display public-key peer brief
Type  Module  Name
---------------------------
RSA   1024    idrsa
DSA   1024    10.1.1.1
```

peer-public-key end

Syntax

peer-public-key end

View

Public key view

Default Level

2: System level

Parameters

None

Description

Use the **peer-public-key end** command to return from public key view to system view.

Related commands: **public-key peer**.

Examples

Exit public key view.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] peer-public-key end
[Sysname]
```

public-key-code begin

Syntax

public-key-code begin

View

Public key view

Default Level

2: System level

Parameters

None

Description

Use the **public-key-code begin** command to enter public key code view.

After entering public key code view, you can input the key in a correct format. Spaces and carriage returns are allowed between characters.

You can input the key data displayed with the **display public-key local public** command so that the format requirements are met.

Related commands: **public-key peer**, **public-key-code end**.

Examples

Enter public key code view and input the key.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] public-key-code begin
[Sysname-pkey-key-code]30819F300D06092A864886F70D010101050003818D0030818902818100C0EC801
4F82515F6335A0A
[Sysname-pkey-key-code]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719D164313
5877E13B1C531B4
[Sysname-pkey-key-code]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952ADF6B80
EB5F52698FCF3D6
[Sysname-pkey-key-code]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4A9B1DDE
675AC30CB020301
[Sysname-pkey-key-code]0001
```

public-key-code end

Syntax

public-key-code end

View

Public key code view

Default Level

2: System level

Parameters

None

Description

Use the **public-key-code end** command to return from public key code view to public key view and to save the configured public key.

The system verifies the key before saving it. If the key contains invalid characters, the system displays an error message and discards the key. Otherwise, the system saves the key.

Related commands: **public-key peer**, **public-key-code begin**.

Examples

Exit public key code view and save the configured public key.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] public-key-code begin
[Sysname-pkey-key-code]30819F300D06092A864886F70D010101050003818D0030818902818100C0EC801
4F82515F6335A0A
[Sysname-pkey-key-code]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719D164313
5877E13B1C531B4
[Sysname-pkey-key-code]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952ADF6B80
EB5F52698FCF3D6
[Sysname-pkey-key-code]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4A9B1DDE
675AC30CB020301
[Sysname-pkey-key-code]0001
[Sysname-pkey-key-code] public-key-code end
[Sysname-pkey-public-key]
```

public-key local create

Syntax

public-key local create { **dsa** | **rsa** }

View

System view

Default Level

2: System level

Parameters

dsa: DSA key pair.

rsa: RSA key pair.

Description

Use the **public-key local create** command to create local key pair(s).

Note that:

- When using this command to create DSA or RSA key pairs, you will be prompted to provide the length of the key modulus. The modulus length is in the range 512 to 2048 bits, and defaults to 1024 bits. If the type of key pair already exists, the system will ask you whether you want to overwrite it.
- The configuration of this command can survive a reboot.

Related commands: **public-key local destroy**, **display public-key local public**.

Examples

Create local RSA key pairs.

```
<Sysname> system-view
[Sysname] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++
++++++
++++++++
++++++++
```

Create a local DSA key pair.

```
<Sysname> system-view
[Sysname] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
*
*
```

public-key local destroy

Syntax

public-key local destroy { **dsa** | **rsa** }

View

System view

Default Level

2: System level

Parameters

dsa: DSA key pair.

rsa: RSA key pair.

Description

Use the **public-key local destroy** command to destroy the local key pair(s).

Related commands: **public-key local create**.

Examples

Destroy the local RSA key pairs.

```
<Sysname> system-view
[Sysname] public-key local destroy rsa
Warning: Confirm to destroy these keys? [Y/N]:y
```

Destroy the local DSA key pair.

```
<Sysname> system-view
[Sysname] public-key local destroy dsa
Warning: Confirm to destroy these keys? [Y/N] :y
```

public-key local export dsa

Syntax

public-key local export dsa { **openssh** | **ssh2** } [*filename*]

View

System view

Default Level

1: Monitor level

Parameters

openssh: Uses the format of OpenSSH.

ssh2: Uses the format of SSH2.0.

filename: Name of the file for storing public key. For detailed information about file name, refer to *File System Management* in the *System Volume.*

Description

Use the **public-key local export dsa** command to display the local DSA public key on the screen or export it to a specified file.

If you do not specify the *filename* argument, the command displays the local DSA public key on the screen; otherwise, the command exports the local DSA public key to the specified file and saves the file.

SSH2.0 and OpenSSH are two different public key formats for different requirements.

Related commands: **public-key local create**, **public-key local destroy**.

Examples

Export the local DSA public key in OpenSSH format to a file named **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh key.pub
```

Display the local DSA public key in SSH2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export dsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-20070625"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBANVcLNEKdDt6xcatpRjxsSrhXFVIdRjx
w59qZnKhl87GsbgP4ccUp3KmcRzuqpz1qNtfgoZOLzHnG1YGxPp7Q2k/uRuuHN0bJfBkOLo2/RyGqDJIqB4FQwmr
kwJuauYGqQy+mgE6dmHn0VG4gAkx9MQxDIBjzbZRX0bvxMdNKR22
---- END SSH2 PUBLIC KEY ----
```

Display the local DSA public key in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACBANVcLNEKdDt6xcatpRjxsSrhXFVIdRjx
w59qZnKhl87GsbgP4ccUp3KmcRzuqpz1qNtfgoZOLzHnG1YGxPp7Q2k/uRuuHN0bJfBkOLo2/RyGqDJIqB4FQwmr
kwJuauYGqQy+mgE6dmHn0VG4gAkx9MQxDIBjzbZRX0bvxMdNKR22 dsa-key
```

public-key local export rsa

Syntax

public-key local export rsa { **openssh** | **ssh1** | **ssh2** } [*filename*]

View

System view

Default Level

1: Monitor level

Parameters

openssh: Uses the format of OpenSSH.

ssh1: Uses the format of SSH1.5.

ssh2: Uses the format of SSH2.0.

filename: Name of the file for storing the public key. For detailed information about file name, refer to *File System Management* in the *System Volume.*

Description

Use the **public-key local export rsa** command to display the local RSA public key on the screen or export them to a specified file.

If you do not specify the *filename* argument, the command displays the local RSA public key on the screen; otherwise, the command exports the local RSA public key to the specified file and saves the file.

SSH1, SSH2.0 and OpenSSH are three different public key formats for different requirements.

Related commands: **public-key local create**, **public-key local destroy**.

Examples

Export the local RSA public key in OpenSSH format to a file named **key.pub**.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh key.pub
```

Display the local RSA public key in SSH2.0 format.

```
<Sysname> system-view
[Sysname] public-key local export rsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20070625"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDAo0dVYR1S5f30eLKGNKuqb5HU3M0TTSaGlER2GmcRI2sgSegbo1x6ut5N
Ic5+jJxuRCU4+gMc76iS8d+2d50FqIweEkHHkSG/ddgXt/iAZ6cY81bdu/CKxGiQlkUpbw4vSv+X5KeE7j+o0MpO
pzh3W768/+u1riz+1LcwVTs51Q==
---- END SSH2 PUBLIC KEY ----
```

Display the local RSA public key in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDAo0dVYR1S5f30eLKGNKuqb5HU3M0TTSaGlER2GmcRI2sgSegbo1x6ut5N
Ic5+jJxuRCU4+gMc76iS8d+2d50FqIweEkHHkSG/ddgXt/iAZ6cY81bdu/CKxGiQlkUpbw4vSv+X5KeE7j+o0MpO
pzh3W768/+u1riz+1LcwVTs51Q== rsa-key
```

public-key peer

Syntax

public-key peer *keyname*

undo public-key peer *keyname*

View

System view

Default Level

2: System level

Parameters

keyname: Public key name, a case-sensitive string of 1 to 64 characters.

Description

Use the **public-key peer** command to configure the public key name and enter public key view.

Use the **undo public-key peer** command to remove a configured peer public key.

After entering public key view, you can configure the public key of the peer with the **public-key-code begin** and **public-key-code end** commands. This requires that you obtain the hexadecimal public key from the peer beforehand.

Related commands: **public-key-code begin**, **public-key-code end**, **display public-key peer**.

Examples

Enter public key view, specifying a public key name of **key1**.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key]
```

public-key peer import sshkey

Syntax

public-key peer *keyname* **import sshkey** *filename*

undo public-key peer *keyname*

View

System view

Default Level

2: System level

Parameters

keyname: Public key name, a case-sensitive string of 1 to 64 characters.

filename: Public key file name. For detailed information about file name, refer to *File System Management* in the *System Volume.*

Description

Use the **public-key peer import sshkey** command to import the public key of a peer from the public key file.

Use the **undo public-key peer** command to remove a configured peer public key.

After execution of this command, the system automatically transforms the public key in SSH1, SSH2.0 or OpenSSH format to PKCS format, and imports the peer public key. This requires that you get a copy of the public key file from the peer through FTP or TFTP in advance.

Related commands: **display public-key peer**.

Examples

Import the peer host public key named **key2** from the public key file **key.pub**.

```
<Sysname> system-view
[Sysname] public-key peer key2 import sshkey key.pub
```

14 ACL Configuration Commands

Common Configuration Commands

display acl resource

Syntax

display acl resource [**slot** *slot number*]

View

Any view

Default Level

1: Monitor level

Parameters

slot *slot-number*: Displays the usage of ACL resources on the specified device in the IRF. If the *slot-number* argument is not specified, the usage on all devices in the IRF is displayed. If no IRF is formed, the usage on the current device is displayed. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF.

Description

Use the **display acl resource** command to display the usage of ACL resources on a switch.

Examples

Display the ACL uses on the switch.

```
<Sysname> display acl resource
 Interface:
   GE1/0/1 to GE1/0/28
-------------------------------------------------------------------------
  Type      Total   Reserved  Configured  Remaining
-------------------------------------------------------------------------
 VFP ACL     1024     0         0          1024
 IFP ACL     4096     0         60         4036
 IFP Meter   2048     0         46         2002
 IFP Counter 2048     0         0          2048
 EFP ACL     512      0         0          512
 EFP Meter   256      0         0          256
 EFP Counter 512      0         0          512
```

Display the ACL uses on all devices in the IRF.

```
<Sysname> display acl resource
Interface:
```

```
   GE1/0/1 to GE1/0/28, XGE1/2/1
-------------------------------------------------------------------------------
 Type      Total   Reserved  Configured  Remaining
-------------------------------------------------------------------------------
VFP ACL    1024    0         0           1024
IFP ACL    4096    0         86          4010
IFP Meter  2048    0         35          2013
IFP Counter 2048   0         35          2013
EFP ACL    512     0         0           512
EFP Meter  256     0         0           256
EFP Counter 512    0         0           512


Interface:
   GE2/0/1 to GE2/0/32, GE2/0/1
-------------------------------------------------------------------------------
 Type      Total   Reserved  Configured  Remaining
-------------------------------------------------------------------------------
VFP ACL    1024    0         0           1024
IFP ACL    4096    0         86          4010
IFP Meter  2048    0         35          2013
IFP Counter 2048   0         35          2013
EFP ACL    512     0         0           512
```

Table 14-1 display acl resource command output description

Field	Description
Interface	Interface indicated by its type and number
Type	Resource type: • ACL indicates ACL rule resources, • Meter indicates traffic policing resources, • Counter indicates traffic statistics resources, • VFP indicates the count of resources that are before Layer 2 forwarding and applied in QinQ, • IFP indicates the count of resources in the inbound direction, • EFP indicates the count of resources in the outbound direction.
Total	Total number of ACLs supported
Reserved	Number of reserved ACLs
Configured	Number of configured ACLs
Remaining	Number of remaining ACLs

display time-range

Syntax

display time-range { *time-range-name* | **all** }

View

Any view

Default Level

1: Monitor level

Parameters

time-range-name: Time range name, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

all: Specifies all existing time ranges.

Description

Use the **display time-range** command to display the configuration and status of a specified time range or all time ranges.

A time range is active if the system time falls into its range.

Examples

Display the configuration and status of time range **trname**.

```
<Sysname> display time-range trname
Current time is 22:20:18 1/5/2006 Thursday
Time-range : trname ( Inactive )
 from 15:00 1/28/2006 to 15:00 1/28/2008
```

Table 14-2 display time-range command output description

Field	Description
Current time	Current system time
Time-range	Configuration and status of the time range, including the name of the time range, its status (active or inactive), and its start time and end time.

time-range

Syntax

time-range *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-range-name* [*start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

View

System view

Default Level

2: System level

Parameters

time-range-name: Time range name, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

start-time: Start time of a periodic time range, in *hh*:*mm* format (24-hour clock), where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 23:59.

end-time: End time of the periodic time range, in *hh*:*mm* format (24-hour clock), where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 24:00. The end time must be greater than the start time.

days: Indicates on which day or days of the week the periodic time range is valid. You may specify multiple values, in words or in digits, separated by spaces, but make sure that they do not overlap. These values can take one of the following forms:

- A digit in the range 0 to 6, respectively for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
- Week in words, that is, Mon, Tue, Wed, Thu, Fri, Sat, or Sun.
- working-day for Monday through Friday.
- off-day for Saturday and Sunday.
- daily for seven days of a week.

from *time1 date1*: Indicates the start time and date of an absolute time range. The *time1* argument specifies the time of the day in *hh*:*mm* format (24-hour clock), where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 23:59. The *date1* argument specifies a date in *MM*/*DD*/*YYYY* or *YYYY*/*MM*/*DD* format, where *MM* is the month of the year in the range 1 to 12, DD is the day of the month in the range 1 to 31, and YYYY is the year in the usual Gregorian calendar in the range 1970 to 2100. If not specified, the start time is the earliest time available in the system, namely, 01/01/1970 00:00:00 AM.

to *time2 date2*: Indicates the end time and date of the absolute time range. The format of the *time2* argument is the same as that of the *time1* argument, but its value ranges from 00:00 to 24:00. The end time must be greater than the start time. If not specified, the end time is the maximum time available in the system, namely, 12/31/2100 24:00:00 PM. The format and value range of the *date2* argument are the same as those of the *date1* argument.

Description

Use the **time-range** command to create a time range.

Use the **undo time-range** command to remove a time range.

You may create a maximum of 256 time ranges.

A time range can be one of the following:

- Periodic time range created using the **time-range** *time-range-name start-time* **to** *end-time days* command. A time range thus created recurs periodically on the day or days of the week.
- Absolute time range created using the **time-range** *time-range-name* { **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* } command. Unlike a periodic time range, a time range thus created does not recur. For example, to create an absolute time range that is active between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the **time-range test from 00:00 01/01/2004 to 23:59 12/31/2004** command.
- Compound time range created using the **time-range** *time-range-name start-time* **to** *end-time days* { **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* } command. A time range thus created recurs on the day or days of the week only within the specified period. For example, to create a time range that is active from 12:00 to 14:00 on Wednesdays between January 1, 2004 00:00 and

December 31, 2004 23:59, you may use the **time-range test 12:00 to 14:00 wednesday from 00:00 01/01/2004 to 23:59 12/31/2004** command.

You may create individual time ranges identified with the same name. They are regarded as one time range whose active period is the result of ORing periodic ones, ORing absolute ones, and ANDing periodic and absolute ones.

Examples

Create an absolute time range named **test**, setting it to become active from 00:00 on January 1, 2008.

```
<Sysname> system-view
[Sysname] time-range test from 0:0 2008/1/1
```

Create a periodic time range named **test**, setting it to be active between 8:00 to 18:00 during working days.

```
<Sysname> system-view
[Sysname] time-range test 8:00 to 18:00 working-day
```

Create a periodic time range named **test**, setting it to be active between 14:00 and 18:00 on Saturday and Sunday.

```
<Sysname> system-view
[Sysname] time-range test 14:00 to 18:00 off-day
```

IPv4 ACL Configuration Commands

acl

Syntax

acl number *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]

undo acl { **all** | **name** *acl-name* | **number** *acl-number* }

View

System view

Default Level

2: System level

Parameters

number *acl-number*: Specifies the number of the IPv4 ACL, which must be in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

name *acl-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

match-order: Specifies the order in which ACL rules are matched.

- **auto**: Performs depth-first match.
- **config**: Performs matching against rules in the order in which they are configured.

all: Specifies all IPv4 ACLs.

Description

Use the **acl** command to enter IPv4 ACL view. If the ACL does not exist, it is created first.

Use the **undo acl** command to remove a specified IPv4 ACL or all IPv4 ACLs.

By default, the match order is **config**.

Note that:

- You can specify a name for an IPv4 ACL only when you create the ACL. After creating an ACL, you cannot specify a name for it, nor can you change or remove its name.
- The name of an IPv4 ACL must be unique among IPv4 ACLs. However, an IPv4 ACL and an IPv6 ACL can share the same name.
- If you specify both an ACL number and an ACL name in one command to enter the view of an existing ACL, be sure that the ACL number and ACL name identify the same ACL.
- You can also use this command to modify the match order of an existing ACL but only when the ACL does not contain any rules.

Examples

Create IPv4 ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

Create IPv4 ACL 2002, naming it **flow**.

```
<Sysname> system-view
[Sysname] acl number 2002 name flow
[Sysname-acl-basic-2002-flow]
```

Enter the view of an unnamed IPv4 ACL by specifying its number.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

Enter the view of a named IPv4 ACL by specifying its number.

```
<Sysname> system-view
[Sysname] acl number 2002
[Sysname-acl-basic-2002-flow]
```

Delete the IPv4 ACL numbered 2000.

```
<Sysname> system-view
[Sysname] undo acl number 2000
```

Delete the IPv4 ACL named **flow**.

```
<Sysname> system-view
[Sysname] undo acl name flow
```

acl copy

Syntax

acl copy { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

View

System view

Default Level

2: System level

Parameters

source-acl-number: Number of an existing IPv4 ACL, which must be in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

name *source-acl-name*: Name of an existing IPv4 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

dest-acl-number: Number of a non-existent IPv4 ACL, which must be of the same ACL type as the source ACL and in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

name *dest-acl-name*: Name of a non-existent IPv4 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion. The system will automatically assign the new ACL a number which is the smallest among the available numbers of the same ACL type.

Description

Use the **acl copy** command to create an IPv4 ACL by copying an existing IPv4 ACL. The new ACL is of the same ACL type and has the same match order, rules, rule numbering step and descriptions.

Note that:

- The source IPv4 ACL and the destination IPv4 ACL must be of the same type.
- The new ACL does not take the name of the source IPv4 ACL.

Examples

Copy ACL 2008 to generate ACL 2009.

```
<Sysname> system-view
[Sysname] acl copy 2008 to 2009
```

acl name

Syntax

acl name *acl-name*

View

System view

Default Level

2: System level

Parameters

acl-name: Name of the IPv4 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Description

Use the **acl name** command to enter the view of an existing IPv4 ACL by specifying its name.

Examples

Enter the view of the IPv4 ACL named **flow**.

```
<Sysname> system-view
[Sysname] acl name flow
[Sysname-acl-basic-2002-flow]
```

description (for IPv4)

Syntax

description *text*

undo description

View

Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view

Default Level

2: System level

Parameters

text: ACL description, a case-sensitive string of 1 to 127 characters.

Description

Use the **description** command to configure a description for an IPv4 ACL to, for example, describe the purpose of the ACL.

Use the **undo description** command to remove the ACL description.

By default, an IPv4 ACL has no ACL description.

Examples

Configure a description for IPv4 ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] description This acl is used in geth 1/0/1
```

Configure a description for IPv4 ACL 3000.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] description This acl is used in geth 1/0/1
```

Configure a description for ACL 4000.

```
<Sysname> system-view
```

```
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] description This acl is used in geth 1/0/1
```

display acl

Syntax

display acl { *acl-number* | **all** | **name** *acl-name* }

View

Any view

Default Level

1: Monitor level

Parameters

acl-number: IPv4 ACL number, which must be in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

all: Specifies all IPv4 ACLs.

name *acl-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Description

Use the **display acl** command to display information about a specified IPv4 ACL or all IPv4 ACLs.

Note that this command displays ACL rules in the match order.

Examples

Display information about IPv4 ACL 2001.

```
<Sysname> display acl 2001
Basic ACL  2001, named flow, 1 rule,
ACL's step is 5
 rule 5 permit source 1.1.1.1 0 (5 times matched)
 rule 5 comment This rule is used in geth 1/0/1
```

Table 14-3 display acl command output description

Field	Description
Basic ACL 2001	The displayed information is about basic IPv4 ACL 2001.
named flow	The name of the ACL is flow.
1 rule	The ACL contains one rule.
ACL's step is 5	The rule numbering step is 5.
5 times matched	There have been five matches for the rule. Only ACL matches performed by software are counted. This field is not displayed when no match is found.

Field	Description
rule 5 comment This rule is used in geth 1/0/1	The description of ACL rule 5 is “This rule is used in geth 1/0/1.”

reset acl counter

Syntax

reset acl counter { *acl-number* | **all** | **name** *acl-name* }

View

User view

Default Level

2: System level

Parameters

acl-number: IPv4 ACL number, which must be in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

all: Specifies all IPv4 ACLs except for user-defined ACLs.

name *acl-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Description

Use the **reset acl counter** command to clear statistics on a specified IPv4 ACL or all IPv4 ACLs that are referenced by upper layer software.

Examples

Clear statistics on IPv4 ACL 2001.

```
<Sysname> reset acl counter 2001
```

Clear statistics on IPv4 ACL **flow**.

```
<Sysname> reset acl counter name flow
```

rule (basic IPv4 ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [**fragment** | **logging** | **source** | **time-range** | **vpn-instance**] *

View

Basic IPv4 ACL view

Default Level

2: System level

Parameters

rule-id: Basic IPv4 ACL rule number, in the range 0 to 65534.

deny: Drops matched packets.

permit: Allows matched packets to pass.

fragment: Indicates that the rule applies to only non-first fragments. A rule without this keyword applies to all fragments and non-fragments.

logging: Generates log entries for matched packets. This function requires that the module using the ACL support logging.

source { *sour-addr sour-wildcard* | **any** }: Specifies a source address. The *sour-addr sour-wildcard* argument combination specifies a source IP address in dotted decimal notation. A wildcard of zero indicates a host address. The **any** keyword indicates any source IP address.

time-range *time-range-name*: Specifies the time range in which the rule takes effect. The *time-range-name* argument is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Without this combination, the rule applies to only non-VPN packets.

Description

Use the **rule** command to create a basic IPv4 ACL rule or modify an existing basic IPv4 ACL rule.

Use the **undo rule** command to remove a basic IPv4 ACL rule or remove some criteria from the rule.

If you specify no optional keywords, the **undo rule** command removes the entire ACL rule; otherwise, the command removes only the specified criteria. Before performing the **undo rule** command, you may use the **display acl** command to view the ID of the rule.

When defining ACL rules, you do not need to assign them IDs; the system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is the smallest multiple of the step that is bigger than the current biggest number. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.

You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

Note

For a basic IPv4 ACL rule to be referenced by a QoS policy for traffic classification, the **logging** keyword is not supported.

Related commands: **display acl**.

Examples

Create a rule to deny packets with the source IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 1.1.1.1 0
```

rule (advanced IPv4 ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ **established** | { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * } | **destination** { *dest-addr dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **fragment** | **icmp-type** { *icmp-type icmp-code* | *icmp-message* } | **logging** | **precedence** *precedence* | **reflective** | **source** { *sour-addr sour-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **tos** *tos* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [{ **established** | { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * } | **destination** | **destination-port** | **dscp** | **fragment** | **icmp-type** | **logging** | **precedence** | **reflective** | **source** | **source-port** | **time-range** | **tos** | **vpn-instance**] *

View

Advanced IPv4 ACL view

Default Level

2: System level

Parameters

rule-id: Advanced IPv4 ACL rule number, in the range 0 to 65534.

deny: Drops matched packets.

permit: Allows matched packets to pass.

protocol: Protocol carried by IP. It can be a number in the range 0 to 255, or in words, **gre** (47), **icmp** (1), **igmp** (2), **ip**, **ipinip** (4), **ospf** (89), **tcp** (6), or **udp** (17). Table 14-4 shows the parameters that can be specified after the *protocol* argument.

Table 14-4 Match criteria and other rule information for advanced IPv4 ACL rules

Parameters	Function	Description
source { *sour-addr sour-wildcard* | **any** }	Specifies a source address.	The *sour-addr sour-wildcard* argument combination specifies a source IP address in dotted decimal notation. A wildcard of zero indicates a host address. The **any** keyword indicates any source IP address.
destination { *dest-addr dest-wildcard* | **any** }	Specifies a destination address.	The *dest-addr dest-wildcard* argument combination specifies a destination IP address in dotted decimal notation. A wildcard of zero indicates a host address. The **any** keyword indicates any destination IP address.
precedence *precedence*	Specifies an IP precedence value.	The *precedence* argument can be a number in the range 0 to 7, or in words, **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), or **network** (7).
tos *tos*	Specifies a ToS preference.	The *tos* argument can be a number in the range 0 to 15, or in words, **max-reliability** (2), **max-throughput** (4), **min-delay** (8), **min-monetary-cost** (1), or **normal** (0).
dscp *dscp*	Specifies a DSCP priority.	The *dscp* argument can be a number in the range 0 to 63, or in words, **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
logging	Specifies to log matched packets.	This function requires that the module using the ACL support logging.
reflective	Specifies that the rule be reflective.	A rule with the **reflective** keyword can be defined only for TCP, UDP, or ICMP packets and can only be a permit statement.
vpn-instance *vpn-instance-name*	Specifies a VPN instance.	The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. Without this combination, the rule applies to only non-VPN packets.
fragment	Indicates that the rule applies to only non-first fragments.	Without this keyword, the rule applies to all fragments and non-fragments.
time-range *time-range-name*	Specifies the time range in which the rule takes effect.	The *time-range-name* argument is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Setting the *protocol* argument to **tcp** or **udp**, you may define the parameters shown in Table 14-5.

Table 14-5 TCP/UDP-specific parameters for advanced IPv4 ACL rules

Parameters	Function	Description
source-port *operator port1* [*port2*]	Specifies one or more UDP or TCP source ports.	The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), **neq** (not equal to), or **range** (inclusive range). The *port1* and *port2* arguments are TCP or UDP port numbers in the range 0 to 65535. *port2* is needed only when the *operator* argument is **range**. TCP port numbers can be represented in these words: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), and **www** (80). UDP port numbers can be represented in these words: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), and **xdmcp** (177). With the **range** operator, the value of *port2* does not need to be greater than that of *port1* because the switch can automatically judge the value range. If the two values are the same, the switch will convert the operator **range** to **eq**. Note that if you specify a combination of **lt** 1 or **gt** 65534, the switch will convert it to **eq** 0 or **eq** 65535.
destination-port *operator port1* [*port2*]	Specifies one or more UDP or TCP destination ports.	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	Specifies one or more TCP flags	Parameters specific to TCP. The value for each argument can be 0 or 1. If multiple TCP flags are specified in the rule, they are in the AND relation.
established	Specifies TCP flags ACK and RST	With the keyowrd, the rule applies to pakets with the value of the ACK or RST flag being 1.

Setting the *protocol* argument to **icmp**, you may define the parameters shown in Table 14-6.

Table 14-6 ICMP-specific parameters for advanced IPv4 ACL rules

Parameters	Function	Description
icmp-type { *icmp-type* *icmp-code* | *icmp-message* }	Specifies the ICMP message type and code.	The *icmp-type* argument ranges from 0 to 255. The *icmp-code* argument ranges from 0 to 255. The *icmp-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 14-7.

Table 14-7 ICMP message names supported in advanced IPv4 ACL rules

ICMP message name	Type	Code
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

Description

Use the **rule** command to create an advanced IPv4 ACL rule or modify an existing advanced IPv4 ACL rule.

Use the **undo rule** command to remove an advanced IPv4 ACL rule or remove some criteria from the rule.

If you specify no optional keywords, the **undo rule** command removes the entire ACL rule; otherwise, the command removes only the specified criteria. Before performing the **undo rule** command, you may use the **display acl** command to view the ID of the rule.

When defining ACL rules, you do not need to assign them IDs; the system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is the smallest multiple of the step that is bigger than the current biggest number. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.

You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

If the ACL match order is **auto**, rules are displayed in the depth-first match order rather than by rule number.

 **Note**

For an advanced IPv4 ACL to be referenced by a QoS policy for traffic classification:

- The **logging** and **reflective** keywords are not supported.
- The operator cannot be **neq** if the ACL is for the inbound traffic.
- The operator cannot be **gt**, **lt**, **neq**, or **range** if the ACL is for the outbound traffic.

Related commands: **display acl**.

Examples

Define a rule to permit TCP packets with the destination port of 80 from 129.9.0.0 to 202.38.160.0.

```
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-adv-3101] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0
0.0.0.255 destination-port eq 80
```

rule (Ethernet frame header ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **dest-mac** *dest-addr dest-mask* | **lsap** *lsap-code lsap-wildcard* | **source-mac** *sour-addr source-mask* | **time-range** *time-range-name* | **type** *type-code type-wildcard*] *

undo rule *rule-id*

View

Ethernet frame header ACL view

Default Level

2: System level

Parameters

rule-id: Ethernet frame header ACL rule number, in the range 0 to 65534.

deny: Drops matched packets.

permit: Allows matched packets to pass.

cos *vlan-pri:* Defines an 802.1p priority. The *vlan-pri* argument can be a number in the range 0 to 7 or in words, **best-effort** (0), **background** (1), **spare** (2), **excellent-effort** (3), **controlled-load** (4), **video** (5), **voice** (6), or **network-management** (7).

dest-mac *dest-addr dest-mask:* Specifies a destination MAC address range. The *dest-addr* and *dest-mask* arguments indicate a destination MAC address and mask in xxxx-xxxx-xxxx format.

lsap *lsap-code lsap-wildcard:* Defines the DSAP and SSAP fields in the LLC encapsulation. The *lsap-code* argument is a 16-bit hexadecimal number indicating the frame encapsulation. The *lsap-wildcard* argument is a 16-bit hexadecimal number indicating the wildcard of the LSAP code. Support for this keyword and argument combination depends on the device model.

source-mac *sour-addr source-mask:* Specifies a source MAC address range. The *sour-addr* and *sour-mask* arguments indicate a source MAC address and mask in xxxx-xxxx-xxxx format.

time-range *time-range-name*: Specifies the time range in which the rule takes effect. The *time-range-name* argument is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

type *type-code type-wildcard:* Defines a link layer protocol. The *type-code* argument is a 16-bit hexadecimal number indicating the frame type. It corresponds to the type-code field in Ethernet_II and Ethernet_SNAP frames. The *type-wildcard* argument is a 16-bit hexadecimal number indicating the wildcard. Support for this keyword and argument combination depends on the device model.

Description

Use the **rule** command to create an Ethernet frame header ACL rule or modify an existing Ethernet frame header ACL rule.

Use the **undo rule** command to remove an Ethernet frame header ACL rule.

When defining ACL rules, you do not need to assign them IDs; the system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is the smallest multiple of the step that is bigger than the current biggest number. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

Before performing the **undo rule** command to remove an Ethernet frame header ACL rule, you may use the **display acl** command to view the ID of the rule.

You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.

You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

If the ACL match order is **auto**, rules are displayed in the depth-first match order rather than by rule number.

Note

For an Ethernet frame header ACL to be referenced by a QoS policy for traffic classification, the **lsap** keyword is not supported.

Related commands: **display acl**.

Examples

Create a rule to deny packets with the 802.1p priority of 3.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule deny cos 3
```

rule comment (for IPv4)

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

View

Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view

Default Level

2: System level

Parameters

rule-id: IPv4 ACL rule number, in the range 0 to 65534.

text: IPv4 ACL rule description, a case-sensitive string of 1 to 127 characters.

Description

Use the **rule comment** command to configure a description for an existing IPv4 ACL rule or modify the description of an IPv4 ACL rule. You may use the rule description to, for example, describe the purpose of the ACL rule or the parameters it contains.

Use the **undo rule comment** command to remove the ACL rule description.

By default, an IPv4 ACL rule has no rule description.

Examples

Create a rule in ACL 2000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 0 deny source 1.1.1.1 0
```

```
[Sysname-acl-basic-2000] rule 0 comment This rule is used in geth 1/0/1
```

Create a rule in ACL 3000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 0 permit ip source 1.1.1.1 0
[Sysname-acl-adv-3000] rule 0 comment This rule is used in geth 1/0/1
```

Create a rule in ACL 4000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule 0 deny cos 3
[Sysname-acl-ethernetframe-4000] rule 0 comment This rule is used in geth 1/0/1
```

step (for IPv4)

Syntax

step *step-value*

undo step

View

Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view

Default Level

2: System level

Parameters

step-value: IPv4 ACL rule numbering step, in the range 1 to 20.

Description

Use the **step** command to set a rule numbering step for an ACL.

Use the **undo step** command to restore the default.

By default, the rule numbering step is five.

Examples

Set the rule numbering step to 2 for ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] step 2
```

Set the rule numbering step to 2 for ACL 3000.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] step 2
```

Set the rule numbering step to 2 for ACL 4000.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] step 2
```

IPv6 ACL Configuration Commands

acl ipv6

Syntax

acl ipv6 number *acl6-number* [**name** *acl6-name*] [**match-order** { **auto** | **config** }]

undo acl ipv6 { **all** | **name** *acl6-name* | **number** *acl6-number* }

View

System view

Default Level

2: System level

Parameters

number *acl6-number*: Specifies the number of the IPv6 ACL, which must be in the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

name *acl6-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

match-order: Specifies the order in which ACL rules are matched.

auto: Performs depth-first match.

config: Performs matching against rules in the order in which they are configured.

all: Specifies all IPv6 ACLs.

Description

Use the **acl ipv6** command to enter IPv6 ACL view. If the ACL does not exist, it is created first.

Use the **undo acl ipv6** command to remove a specified IPv6 ACL or all IPv6 ACLs.

By default, the match order is **config**.

Note that:

- You can specify a name for an IPv6 ACL only when you create the ACL. After creating an ACL, you cannot specify a name for it, nor can you change or remove its name.
- The name of an IPv6 ACL must be unique among IPv6 ACLs. However, an IPv4 ACL and an IPv6 ACL can share the same name.
- If you specify both an ACL number and an ACL name in one command to enter the view of an existing ACL, be sure that the ACL number and ACL name identify the same ACL.
- You can also use this command to modify the match order of an existing IPv6 ACL, but only when the ACL does not contain any rules.

Examples

Create IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000]
```

Create IPv6 ACL 2002, giving the ACL a name of flow.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2002 name flow
[Sysname-acl6-basic-2002-flow]
```

Enter the view of an IPv6 ACL that has no name by specifying its number.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000]
```

Enter the view of an IPv6 ACL that has a name by specifying its number.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2002
[Sysname-acl6-basic-2002-flow]
```

Delete the IPv6 ACL with the number of 2000.

```
<Sysname> system-view
[Sysname] undo acl ipv6 number 2000
```

Delete the IPv6 ACL named flow.

```
<Sysname> system-view
[Sysname] undo acl ipv6 name flow
```

acl ipv6 copy

Syntax

acl ipv6 copy { *source-acl6-number* | **name** *source-acl6-name* } **to** { *dest-acl6-number* | **name** *dest-acl6-name* }

View

System view

Default Level

2: System level

Parameters

source-acl6-number: Number of an existing IPv6 ACL, which must be in the following ranges:

- 2000 to 2999 for basic IPv6 ACLs,
- 3000 to 3999 for advanced IPv6 ACLs.

name *source-acl6-name*: Name of an existing IPv6 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

dest-acl6-number: Number of a non-existent IPv6 ACL, which must be in the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

name *dest-acl6-name*: Name for the new IPv6 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion. The system will automatically assign the new ACL a number which is the smallest one among the available numbers of the same ACL type.

Description

Use the **acl ipv6 copy** command to create an IPv6 ACL by copying an existing IPv6 ACL. The new ACL is of the same ACL type and has the same match order, rules, rule numbering step and descriptions.

Note that:

- The source IPv6 ACL and the destination IPv6 ACL must be of the same type.
- The new ACL does not take the name of the source IPv6 ACL.

Examples

Copy ACL 2008 to generate ACL 2009.

```
<Sysname> system-view
[Sysname] acl ipv6 copy 2008 to 2009
```

acl ipv6 name

Syntax

acl ipv6 name *acl6-name*

View

System view

Default Level

2: System level

Parameters

acl6-name: Name of the IPv6 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Description

Use the **acl ipv6 name** command to enter the view of an existing IPv6 ACL by specifying its name.

Examples

Enter the view of the IPv6 ACL named flow.

```
<Sysname> system-view
[Sysname] acl ipv6 name flow
[Sysname-acl6-basic-2002-flow]
```

description (for IPv6)

Syntax

description *text*

undo description

View

Basic IPv6 ACL view, advanced IPv6 ACL view

Default Level

2: System level

Parameters

text: ACL description, a case-sensitive string of 1 to 127 characters.

Description

Use the **description** command to configure a description for an IPv6 ACL to, for example, describe the purpose of the ACL.

Use the **undo description** command to remove the IPv6 ACL description.

By default, an IPv6 ACL has no ACL description.

Examples

Configure a description for IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] description This acl is used in geth 1/0/1
```

Configure a description for IPv6 ACL 3000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] description This acl is used in geth 1/0/1
```

display acl ipv6

Syntax

display acl ipv6 { *acl6-number* | **all** | **name** *acl6-name* }

View

Any view

Default Level

1: Monitor level

Parameters

acl6-number: IPv6 ACL number, which must be in the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

all: Specifies all IPv6 ACLs.

name *acl6-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Description

Use the **display acl ipv6** command to display information about a specified IPv6 ACL or all IPv6 ACLs.

Note that this command displays ACL rules in the match order.

Examples

Display information about IPv6 ACL 2001.

```
<Sysname> display acl ipv6 2001
Basic IPv6 ACL  2001, named flow, 1 rule,
ACL's step is 5
rule 0 permit source 1::2/128 (5 times matched)
rule 0 comment This rule is used in geth 1/0/1
```

Table 14-8 display acl ipv6 command output description

Field	Description
Basic IPv6 ACL 2001	The displayed information is about basic IPv6 ACL 2001.
named flow	The name of the ACL is flow.
1 rule	The ACL contains one rule.
ACL's step is 5	The rules in this ACL are numbered in steps of 5.
5 times matched	There have been five matches for the rule. Only ACL matches performed by software are counted. This field is not displayed when no match is found.
rule 0 comment This rule is used in geth 1/0/1	The description of ACL rule 0 is “This rule is used in geth 1/0/1.”

reset acl ipv6 counter

Syntax

reset acl ipv6 counter { *acl6-number* | **all** | **name** *acl6-name* }

View

User view

Default Level

2: System level

Parameters

acl6-number: IPv6 ACL number, which must be in the following ranges:

- 2000 to 2999 for basic IPv6 ACLs,
- 3000 to 3999 for advanced IPv6 ACLs.

all: Specifies all basic and advanced IPv6 ACLs.

name *acl6-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Description

Use the **reset acl ipv6 counter** command to clear statistics on a specified IPv6 ACL or all basic and advanced IPv6 ACLs.

Examples

Clear the statistics on IPv6 ACL 2001, which is referenced by upper layer software.

```
<Sysname> reset acl ipv6 counter 2001
```

Clear the statistics on IPv6 ACL flow, which is referenced by upper layer software.

```
<Sysname> reset acl ipv6 counter name flow
```

rule (basic IPv6 ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**fragment** | **logging** | **source** | **time-range**] *

View

Basic IPv6 ACL view

Default Level

2: System level

Parameters

rule-id: IPv6 ACL rule number, in the range 0 to 65534.

deny: Drops matched packets.

permit: Allows matched packets to pass.

fragment: Indicates that the rule applies to only non-first fragments. A rule without this keyword applies to all fragments and non-fragments.

logging: Logs matched packets. This function requires that the module using the ACL support logging.

source { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* | **any** }: Specifies a source address. The *ipv6-address* and *prefix-length* arguments specify a source IPv6 address and its address prefix length in the range 1 to 128. The **any** keyword indicates any IPv6 source address.

time-range *time-range-name*: Specifies the time range in which the rule takes effect. The *time-range-name* argument is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Description

Use the **rule** command to create a basic IPv6 ACL rule or modify an existing basic IPv6 ACL rule.

Use the **undo rule** command to remove a basic IPv6 ACL rule or remove some criteria from the rule.

If you specify no optional keywords, the **undo rule** command removes the entire ACL rule; otherwise, the command removes only the specified criteria. Before performing the **undo rule** command, you may need to use the **display acl ipv6** command to view the ID of the rule.

When defining ACL rules, you do not need to assign them IDs; the system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is the smallest multiple of the step that is bigger than the current biggest number. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.

You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

 **Note**

For a basic IPv6 ACL to be referenced by a QoS policy for traffic classification, the **logging** and **fragment** keywords are not supported.

Related commands: **display acl ipv6**.

Examples

Create IPv6 ACL 2000 and add two rules.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2030:5060::9050/64
[Sysname-acl6-basic-2000] rule 8 deny source fe80:5060::8050/96
```

rule (advanced IPv6 ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ **established** | { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * } | **destination** { *dest dest-prefix* | *dest/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **source** { *source source-prefix* | *source/source-prefix* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

undo rule *rule-id* [{ **established** | { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * } | **destination** | **destination-port** | **dscp** | **fragment** | **icmpv6-type** | **logging** | **source** | **source-port** | **time-range**] *

View

Advanced IPv6 ACL view

Default Level

2: System level

Parameters

rule-id: IPv6 ACL rule number, in the range 0 to 65534.

deny: Drops matched packets.

permit: Allows matched packets to pass.

protocol: Protocol carried over IPv6. It can be a number in the range 0 to 255, or in words, **gre** (47), **icmpv6** (58), **ipv6**, **ipv6-ah** (51), **ipv6-esp** (50), **ospf** (89), **tcp** (6), or **udp** (17). Table 14-9 shows the parameters that can be specified after the *protocol* argument.

Table 14-9 Match criteria and other rule information for advanced IPv6 ACL rules

Parameters	Function	Description
source { *source source-prefix* | *source/source-prefix* | **any** }	Specifies a source IPv6 address.	The *source* and *source-prefix* arguments specify an IPv6 source address and its prefix length in the range 1 to 128. The **any** keyword indicates any IPv6 source address.
destination { *dest dest-prefix* | *dest/dest-prefix* | **any** }	Specifies a destination IPv6 address.	The *dest* and *dest-prefix* arguments specify a destination IPv6 address, and its prefix length in the range 1 to 128. The **any** keyword indicates any IPv6 destination address.
dscp *dscp*	Specifies a DSCP preference	The *dscp* argument can be a number in the range 0 to 63, or in words, **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
logging	Specifies to log matched packets	This function requires that the module using the ACL support logging.
fragment	Indicates that the rule applies to only non-first fragments.	Without this keyword, the rule applies to all fragments and non-fragments.
time-range *time-range-name*	Specifies the time range in which the rule takes effect.	The *time-range-name* argument is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Setting the *protocol* argument to **tcp** or **udp**, you may define the parameters shown in Table 14-10.

Table 14-10 TCP/UDP-specific parameters for advanced IPv6 ACL rules

Parameters	Function	Description
source-port *operator port1* [*port2*]	Specifies one or more UDP or TCP source ports.	The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), **neq** (not equal to), or **range** (inclusive range). The *port1* and *port2* arguments are TCP or UDP port numbers in the range 0 to 65535. *port2* is needed only when the *operator* argument is **range**. TCP port numbers can be represented in these words: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), and **www** (80). UDP port numbers can be represented in these words: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), and **xdmcp** (177). With the **range** operator, the value of *port2* does not need to be greater than that of *port1* because the switch can automatically judge the value range. If the two values are the same, the switch will convert the operator **range** to **eq**. Note that if you specify a combination of **lt** 1 or **gt** 65534, the switch will convert it to **eq** 0 or **eq** 65535.
destination-port *operator port1* [*port2*]	Specifies one or more UDP or TCP destination ports.	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	Specifies one or more TCP flags.	Parameters specific to TCP. The value for each argument can be 0 or 1. If multiple TCP flags are specified in the rule, they are in the AND relation.
established	Specifies TCP flags ACK and RST	With the keyowrd, the rule applies to pakets with the value of the ACK or RST flag being 1.

Setting the *protocol* argument to **icmpv6**, you may define the parameters shown in Table 14-11.

Table 14-11 ICMPv6-specific parameters for advanced IPv6 ACL rules

Parameters	Function	Description
icmpv6-type { *icmpv6-type icmpv6-code* | *icmpv6-message* }	Specifies the ICMPv6 message type and code.	The *icmpv6-type* argument ranges from 0 to 255. The *icmpv6-code* argument ranges from 0 to 255. The *icmpv6-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 14-12.

Table 14-12 ICMPv6 message names supported in advanced IPv6 ACL rules

ICMPv6 message name	Type	Code
redirect	137	0
echo-request	128	0
echo-reply	129	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

Description

Use the **rule** command to create an advanced IPv6 ACL rule or modify an existing advanced IPv6 ACL rule.

Use the **undo rule** command to remove an advanced IPv6 ACL rule or remove some criteria from the rule.

If you specify no optional keywords, the **undo rule** command removes the entire ACL rule; otherwise, the command removes only the specified criteria. Before performing the **undo rule** command, you may need to use the **display acl ipv6** command to view the ID of the rule.

When defining ACL rules, you do not need to assign them IDs; the system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is the smallest multiple of the step that is bigger than the current biggest number. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30.

You cannot create a rule with, or modify a rule to have, the same permit/deny statement as an existing rule in the ACL.

You can only modify the existing rules of an ACL that uses the match order of **config**. When modifying a rule of such an ACL, you may choose to change just some of the settings, in which case the other settings remain the same.

When the ACL match order is **auto**, a newly created rule will be inserted among the existing rules in the depth-first match order. Note that the IDs of the rules still remain the same.

Note

For an advanced IPv6 ACL to be referenced by a QoS policy for traffic classification,

- The **logging** and **fragment** keywords are not supported.
- The operator cannot be **neq** if the ACL is for the inbound traffic.
- The operator cannot be **gt**, **lt**, **neq**, or **range** if the ACL is for the outbound traffic.

Related commands: **display acl ipv6**.

Examples

Configure IPv6 ACL 3000 to permit TCP packets with the source address of 2030:5060::9050/64.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit tcp source 2030:5060::9050/64
```

rule comment (for IPv6)

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

View

Basic IPv6 ACL view, advanced IPv6 ACL view

Default Level

2: System level

Parameters

rule-id: IPv6 ACL rule number, in the range 0 to 65534.

text: IPv6 ACL rule description, a case-sensitive string of 1 to 127 characters.

Description

Use the **rule comment** command to configure a description for an existing IPv6 ACL rule or modify the description of an IPv6 ACL rule. You may use the rule description to, for example, describe the purpose of the ACL rule.

Use the **undo rule comment** command to remove the IPv6 ACL rule description.

By default, an IPv6 ACL rule has no rule description.

Examples

Define a rule in IPv6 ACL 2000 and create a description for the rule.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule 0 permit source 2030:5060::9050/64
[Sysname-acl6-basic-2000] rule 0 comment This rule is used in geth 1/0/1
```

Define a rule in IPv6 ACL 3000 and create a description for the rule.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 0 permit tcp source 2030:5060::9050/64
[Sysname-acl6-adv-3000] rule 0 comment This rule is used in geth 1/0/1
```

step (for IPv6)

Syntax

step *step-value*

undo step

View

Basic IPv6 ACL view, advanced IPv6 ACL view

Default Level

2: System level

Parameters

step-value: IPv6 ACL rule numbering step, in the range 1 to 20.

Description

Use the **step** command to set a rule numbering step for an IPv6 ACL.

Use the **undo step** command to restore the default.

By default, the rule numbering step is five.

Examples

Set the rule numbering step to 2 for IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] step 2
```

Set the rule numbering step to 2 for IPv6 ACL 3000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] step 2
```

ACL Application Commands

acl logging frequence

Syntax

acl logging frequence *frequence*

undo acl logging frequence

View

System view

Default Level

2: System level

Parameters

frequence: Interval in minutes for packet filtering statistics. It must be an integer in the range of 0 to 1440 and a multiple of five.

Description

Use the **acl logging frequence** command to set the interval for IPv4 packet filtering statistics. At the specified interval, the device outputs the statistics information, including the number of filtered packets, and the ACL rules used.

Use the **undo acl logging frequence** command to restore the default.

By default, the interval is 0, that is, no IPv4 packet filtering statistics is collected.

Examples

Set the interval for IPv4 packet filtering statistics to 10 minutes.

```
<Sysname> system-view
[Sysname] acl logging frequence 10
```

acl ipv6 logging frequence

Syntax

acl ipv6 logging frequence *frequence*

undo acl ipv6 logging frequence

View

System view

Default Level

2: System

Parameters

frequence: Interval in minutes for packet filtering statistics. It must be an integer in the range of 0 to 1440 and a multiple of five.

Description

Use the **acl ipv6 logging frequence** command to set the interval for IPv6 packet filtering statistics. At the specified interval, the device outputs the statistics information, including the number of filtered packets, and the ACL rules used.

Use the **undo ipv6 acl logging frequence** command to restore the default.

By default, the interval is 0, that is, no IPv6 packet filtering statistics is collected.

Example

Set the interval for IPv6 packet filtering statistics to 15 minutes.

```
<Sysname> system-view
[Sysname] acl ipv6 logging frequence 15
```

packet-filter

Syntax

packet-filter { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

undo packet-filter { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

View

Ethernet interface view, VLAN interface view

Default Level

2: System level

Parameters

acl-number: Specifies the number of an ACL, which must be in the following ranges:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

name *acl-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

inbound: Specifies to filter the packets received by the interface.

outbound: Specifies to filter the packets that are to be sent out of the interface.

Description

Use the **packet-filter** command to apply an ACL to an interface to filter IPv4 packets or Ethernet frames.

Use the **undo packet-filter** command to restore the default.

By default, an interface does not filter packets and Ethernet frames.

Note that you can apply only one IPv4 ACL or one Ethernet frame header ACL on an interface. To modify the ACL configured on an interface, you need to remove the previous configuration first and then configure a new ACL.

Examples

Apply basic IPv4 ACL 2001 to the inbound direction of interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEtherhet1/0/1] ethernet-frame-filter 2001 inbound
```

Apply advanced IPv4 ACL 3001 to the inbound direction of VLAN interface 10.

```
<Sysname> system-view
[Sysname] interface Vlan-interface 10
[Sysname-Vlan-interface10] ethernet-frame-filter 3001 inbound
```

packet-filter ipv6

Syntax

packet-filter ipv6 { *acl6-number* | **name** *acl6-name* } { **inbound** | **outbound** }

undo packet-filter ipv6 { **inbound** | **outbound** }

View

Interface view

Default Level

2: System level

Parameters

acl6-number: Specifies the number of a basic or advanced IPv6 ACL, which must be in the range of 2000 to 3999.

name *acl6-name*: Specifies the name of the basic or advanced IPv6 ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

inbound: Specifies to filter the IPv6 packets received by the interface

outbound: Specifies to filter the IPv6 packets that are to be sent out of the interface

Description

Use the **packet-filter ipv6** command to apply a basic or advanced IPv6 ACL to an interface to filter IPv6 packets.

Use the **undo packet-filter ipv6** command to restore the default.

By default, an interface does not filter IPv6 packets.

Note that you can apply only one IPv6 ACL on an interface. To modify the ACL configured on an interface, you need to remove the previous configuration first and then configure a new ACL.

Examples

Apply basic IPv6 ACL 2500 to the outbound direction of interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter ipv6 2500 outbound
```

Apply advanced IPv6 ACL 3000 to the outbound direction of interface VLAN interface 20

```
<Sysname> system-view
[Sysname] interface Vlan-interface 20
[Sysname-Vlan-interface20] packet-filter ipv6 3000 outbound
```

Table of Contents

1 Smart Link Configuration Commands

Smart Link Configuration Commands

display smart-link flush

Syntax

display smart-link flush

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display smart-link flush** command to display information about the received flush messages.

Examples

Display information about the received flush messages.

```
<Sysname> display smart-link flush
 Received flush packets                          : 10
 Receiving interface of the last flush packet      : GigabitEthernet1/0/1
 Receiving time of the last flush packet          : 19:19:03 2009/06/27
 Device ID of the last flush packet               : 000f-e200-8500
 Control VLAN of the last flush packet            : 1
```

Table 1-1 display smart-link flush command output description

Field	Description
Received flush packets	Total number of received flush messages
Receiving interface of the last flush packet	The port that received the last flush message
Receiving time of the last flush packet	Time when the last flush message was received
Device ID of the last flush packet	Device ID carried in the last flush message
Control VLAN of the last flush packet	Control VLAN ID carried in the last flush message

display smart-link group

Syntax

display smart-link group { *group-id* | **all** }

View

Any view

Default Level

1: Monitor level

Parameters

group-id: Smart link group ID. The minimum value is 1, while the maximum value is 26.

all: Displays information about all smart link groups.

Description

Use the **display smart-link group** command to display information about the specified or all smart link groups.

Examples

Display information about smart link group 1.

```
<Sysname> display smart-link group 1
 Smart link group 1 information:
 Device ID: 000f-e200-8500
 Preemption mode: ROLE
 Preemption delay: 1(s)
 Control VLAN: 1
 Protected VLAN: Reference Instance 0 to 2, 4
 Member                 Role    State    Flush-count Last-flush-time
 ------------------------------------------------------------------------------
 GigabitEthernet1/0/1     MASTER  ACTVIE   1         16:37:20 2009/04/21
 GigabitEthernet1/0/2     SLAVE   STANDBY  2         17:45:20 2009/04/21
```

Table 1-2 display smart-link group command output description

Field	Description
Smart link group 1 information	Information about smart link group 1
Preemption mode	Preemption mode, which can be **role** for preemption enabled or **none** for preemption disabled.
Preemption delay	Preemption delay time, in seconds
Control-VLAN	Control VLAN ID
Protected VLAN	Protected VLANs of the smart link group. Referenced MSTIs are displayed here. To view the VLANs mapped to the referenced MSTIs, use the **display stp region-configuration** command.
Member	Member port of the smart link group
Role	Port role: master or slave

Field	Description
State	Port state: active or standby
Flush-count	Number of transmitted flush messages
Last-flush-time	The time when the last flush message was transmitted (NA indicates that no flush message has been transmitted)

flush enable

Syntax

flush enable [**control-vlan** *vlan-id*]

undo flush enable

View

Smart link group view

Default Level

2: System level

Parameters

control-vlan *vlan-id*: Specifies the control VLAN used for transmitting flush messages. The *vlan-id* argument ranges from 1 to 4094.

Description

Use the **flush enable** command to enable flush update.

Use the **undo flush enable** command to disable flush update.

By default, flush update is enabled for smart link groups and VLAN 1 is used for flush message transmission.

Note that, you need to configure different control VLANs for different smart link groups.

Related commands: **smart-link flush enable**.

Examples

Disable flush update for smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] undo flush enable
```

port

Syntax

port *interface-type interface-number* { **master** | **slave** }

undo port *interface-type interface-number*

View

Smart link group view

Default Level

2: System level

Parameters

interface-type interface-number: Port type and port number.

master: Specifies a port as the master port.

slave: Specifies a port as the slave port.

Description

Use the **port** command to assign the specified port as the master or slave port of the current smart link group.

Use the **undo port** command to remove the specified port from the smart link group.

Note that:

- Disable STP and RRPP on the ports you want to add to the smart link group, and make sure that the ports are not member ports of any aggregation group or service loopback group. On the other hand, you cannot enable STP or RRPP on a smart link group member port or assign a smart link group member port to an aggregation group or service loopback group.
- You can assign a port to a smart link group with the **port smart-link group** command in Ethernet interface view or Layer-2 aggregate interface view.

Related commands: **port smart-link group**.

Examples

Configure GigabitEthernet 1/0/1 as the slave port of smart link group 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] port gigabitethernet 1/0/1 slave
```

port smart-link group

Syntax

port smart-link group *group-id* { **master** | **slave** }

undo port smart-link group *group-id*

View

Ethernet interface view, Layer-2 aggregate interface view

Default Level

2: System level

Parameters

group-id: Smart link group ID. The minimum value is 1, while the maximum value is 26.

master: Specifies the port as the master port.

slave: Specifies the port as the slave port.

Description

Use the **port smart-link group** command to configure the current port as a member of the specified smart link group.

Use the **port smart-link group** command to remove the port from the specified smart link group.

Note that:

- Disable STP and RRPP on the ports you want to add to the smart link group, and make sure that the ports are not member ports of any aggregation group or service loopback group. On the other hand, you cannot enable STP or RRPP on a smart link group member port or assign a smart link group member port to an aggregation group or service loopback group.
- You can assign a port to a smart link group with the **port** command in smart link group view.

Related commands: **port**.

Examples

Configure GigabitEthernet 1/0/1 as the master port of smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
[Sysname-GigabitEthernet1/0/1] port smart-link group 1 master
```

Configure Layer-2 aggregate interface 1 as the master port of smart link group 1.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 0
[Sysname-smlk-group1] quit
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] undo stp enable
[Sysname-Bridge-Aggregation1] port smart-link group 1 master
```

preemption delay

Syntax

preemption delay *delay-time*

undo preemption delay

View

Smart link group view

Default Level

2: System level

Parameters

delay-time: Preemption delay (in seconds), in the range of 0 to 300.

Description

Use the **preemption delay** command to set the preemption delay. When role preemption is enabled, after the preemption delay is set, the master port waits for some time before taking over, so as to collaborate with the switchover of upstream devices.

Use the **undo preemption delay** command to restore the default.

By default, the preemption delay is 1 second.

Note that, the preemption delay configuration takes effect only after role preemption is enabled.

Related commands: **preemption mode**.

Examples

Enable role preemption and set the preemption delay to 10 seconds.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1] preemption mode role
[Sysname-smlk-group1] preemption delay 10
```

preemption mode

Syntax

preemption mode role

undo preemption mode

View

Smart link group view

Default Level

2: System level

Parameters

role: Configures the role preemption mode, which enables the master port to preempt the slave port in active state.

Description

Use the **preemption mode** command to enable role preemption.

Use the **undo preemption mode** command to disable role preemption.

By default, role preemption is disabled.

Examples

Enable the role preemption mode.

```
<Sysname> system-view
[Sysname] smart-link group 1
```

```
[Sysname-smlk-group1] preemption mode role
```

protected-vlan

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

View

Smart link group view

Default Level

2: System level

Parameters

reference-instance *instance-id-list*: Specifies the MSTIs to be referenced in the form of *instance-id-list* = { *instance-id* [**to** *instance-id*] }&<1-10>, where the range of the *instance-id* argument is as specified in the command configuring MSTIs and &<1-10> indicates that you can provide up to ten MSTIs or MSTI lists.

Description

Use the **protected-vlan** command to configure protected VLANs for a smart link group by referencing MSTIs. You can use the **display stp region-configuration** command to view the VLANs mapped to the referenced MSTIs.

Use the **undo protected-vlan** command to remove the specified protected VLANs from a smart link group by referencing the specified MSTIs. If no MSTI is specified, all the protected VLANs of the smart link group are removed.

By default, no protected VLAN is configured for a smart link group.

Note that:

- Before assigning ports to a smart link group, configure protected VLANs for the smart link group.
- You can remove all protected VLANs from a smart link group when the group is empty but not after a member port is assigned to it.
- Removing a smart link group also removes its protected VLANs.
- If the VLAN(s) mapped to a referenced MSTI changes, the protected VLAN(s) change accordingly.
- The VLANs that the member ports of a smart link group belong to must be configured as the protected VLANs of the smart link group.

Related commands: **smart-link group**, **display stp region-configuration** in *MSTP Commands* in the *Access Volume*.

Examples

Configure the VLANs mapped to MSTIs 1 through 10 and MSTI 12 as the protected VLANs of smart link group 1.

```
<Sysname> system-view
```

```
[Sysname] smart-link group 1
[Sysname-smlk-group1] protected-vlan reference-instance 1 to 10 12
```

reset smart-link statistics

Syntax

reset smart-link statistics

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **reset smart-link statistics** command to clear the statistics about flush messages.

Examples

Clear the statistics about flush messages.

```
<Sysname> reset smart-link statistics
```

smart-link flush enable

Syntax

smart-link flush enable [**control-vlan** *vlan-id-list*]

undo smart-link flush enable [**control-vlan** *vlan-id-list*]

View

Ethernet interface view, Layer-2 aggregate interface view

Default Level

2: System level

Parameters

control-vlan *vlan-id-list*: Specifies the control VLANs used for receiving flush messages. The *vlan-id-list* is expressed in the form of *vlan-id-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where the *vlan-id* argument ranges from 1 to 4094 and &<1-10> indicates that you can provide up to ten VLAN IDs or VLAN ID lists.

Description

Use the **smart-link flush enable** command to configure a VLAN for receiving flush messages, that is, a receive control VLAN, on a port in Ethernet interface view or on all ports in system view.

Use the **undo smart-link flush enable** command to disable flush message processing.

By default, flush messages are not processed.

Note that:

- If no VLAN is specified, VLAN 1 applies.
- This command cannot be used on member port of an aggregation group or service loopback group.

Related commands: **flush enable**.

Examples

Enable GigabitEthernet 1/0/1 to process the flush messages received in VLAN 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] smart-link flush enable
```

Enable Layer-2 aggregate interface 1 to process the flush messages received in VLAN 1.

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] smart-link flush enable
```

smart-link group

Syntax

smart-link group *group-id*

undo smart-link group *group-id*

View

System view

Default Level

2: System level

Parameters

group-id: Smart link group ID. The minimum value is 1, while the maximum value is 26.

Description

Use the **smart-link group** command to create a smart link group and enter smart link group view.

Use the **undo link-aggregation group** command to remove a smart link group.

Note that a smart link group with member ports cannot be removed.

Examples

Create smart link group 1 and enter smart link group view.

```
<Sysname> system-view
[Sysname] smart-link group 1
[Sysname-smlk-group1]
```

2 Monitor Link Configuration Commands

Monitor Link Configuration Commands

display monitor-link group

Syntax

display monitor-link group { *group-id* | **all** }

View

Any view

Default Level

1: Monitor level

Parameters

group-id: Monitor link group ID, in the range 1 to 16.

all: Specifies all monitor link groups.

Description

Use the **display monitor-link group** command to display information about the specified or all smart link groups.

Examples

Display information about monitor link group 1.

```
<Sysname> display monitor-link group 1
Monitor link group 1 information:
  Group status: DOWN
  Last-up-time: 16:37:20 2009/4/21
  Last-down-time: 16:38:26 2009/4/21
  Member                Role     Status
  --------------------------------------
  GigabitEthernet1/0/1    UPLINK   DOWN
  GigabitEthernet1/0/2    DOWNLINK  DOWN
```

Table 2-1 display monitor-link group command output description

Field	Description
Group status	Monitor link group state, which can be up or down
Last-up-time	Last time when the monitor link group was up
Last-down-time	Last time when the monitor link group was down

Field	Description
Member	Member ports of the monitor link group
Role	Port role, which can be uplink or downlink
Status	Member link state, which can be up or down

monitor-link group

Syntax

monitor-link group *group-id*

undo monitor-link group *group-id*

View

System view

Default Level

2: System level

Parameters

group-id: Monitor link group ID, in the range 1 to 16.

Description

Use the **monitor-link group** command to create a monitor link group and enter monitor link group view. If the specified monitor link group already exists, you enter monitor link group view directly.

Use the **undo monitor-link group** command to remove a monitor link group.

Related commands: **port monitor-link group**, **port**.

Examples

Create monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1]
```

port

Syntax

port *interface-type interface-number* { **uplink** | **downlink** }

undo port *interface-type interface-number*

View

Monitor link group view

Default Level

2: System level

Parameters

interface-type interface-number: Port type and port number.

uplink: Specifies an uplink port.

downlink: Specifies a downlink port.

Description

Use the **port** command to assign a port to the monitor link group.

Use the **undo port** command to remove a port from the monitor link group.

Note

- Both Ethernet ports and Layer-2 aggregate interfaces can be assigned to a monitor link group.
- A port can be assigned to only one monitor link group.
- Alternatively, you can assign a port to a monitor link group with the **port monitor-link group** command in Ethernet interface view or Layer-2 aggregate interface view.

Related commands: **port monitor-link group**.

Examples

Configure member ports for monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] port gigabitethernet 1/0/1 uplink
[Sysname-mtlk-group1] port gigabitethernet 1/0/2 downlink
```

port monitor-link group

Syntax

port monitor-link group *group-id* { **uplink** | **downlink** }

undo port monitor-link group *group-id*

View

Ethernet interface view, Layer-2 aggregate interface view

Default Level

2: System level

Parameters

group-id: Monitor link group ID, in the range 1 to 16.

uplink: Specifies an uplink port.

downlink: Specifies a downlink port.

Description

Use the **port monitor-link group** command to assign the port to the specified monitor link group.

Use the **undo port monitor-link group** command to remove the port from the specified monitor link group.

Note

- Both Ethernet ports and Layer-2 aggregate interfaces can be assigned to a monitor link group.
- A port can be assigned to only one monitor link group.
- Alternatively, you can assign a port to a monitor link group with the **port** command in monitor link group view.

Related commands: **port**.

Examples

Configure GigabitEthernet 1/0/1 as an uplink port of monitor link group 1.

```
<Sysname> system-view
[Sysname] monitor-link group 1
[Sysname-mtlk-group1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port monitor-link group 1 uplink
```

3 RRPP Configuration Commands

RRPP Configuration Commands

control-vlan

Syntax

control-vlan *vlan-id*

undo control-vlan

View

RRPP domain view

Default Level

2: System level

Parameters

vlan-id: Specifies a VLAN as the primary control VLAN for the RRPP domain, in the range 2 to 4093. This VLAN must be one not created yet.

Description

Use the **control-vlan** command to specify the primary control VLAN for the current RRPP domain.

Use the **undo control-vlan** command to remove the control VLANs configured for the current RRPP domain.

Note that:

- When configuring control VLANs for an RRPP domain, you only need to configure the control VLAN for the primary ring, that is, the primary control VLAN. The system will automatically configure the VLAN whose VLAN ID is the primary control VLAN ID plus 1 as the secondary control VLAN for subrings. Like the primary control VLAN, the secondary control VLAN must be one not created yet. For the control VLAN configuration to be successful, you must make sure that the IDs for the two control VLANs have not been assigned yet.
- Before configuring RRPP rings for an RRPP domain, you can delete or modify the control VLANs configured for the RRPP domain. However, after configuring RRPP rings for an RRPP domain, you cannot delete or modify the control VLANs of the domain.
- You cannot use the **undo vlan all** command to delete a control VLAN.

Related commands: **rrpp domain**.

Examples

Configure VLAN 100 as the primary control VLAN of RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
```

```
[Sysname-rrpp-domain1] control-vlan 100
```

display rrpp brief

Syntax

display rrpp brief

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display rrpp brief** command to display the brief RRPP information.

Examples

Display the brief RRPP information.

```
<Sysname> display rrpp brief
Flags for Node Mode :
M -- Master , T -- Transit , E -- Edge , A -- Assistant-Edge
RRPP Protocol Status: Enable
Number of RRPP Domains: 2
Domain ID    : 1
Control VLAN  : Major 5   Sub 6
Protected VLAN: Reference Instance 0 to 2, 4
Hello Timer   : 1  sec  Fail Timer : 3  sec
 Ring  Ring   Node  Primary/Common          Secondary/Edge          Enable
 ID    Level  Mode  Port                  Port                  Status
--------------------------------------------------------------------------------
 1    1     M    GigabitEthernet1/0/1     GigabitEthernet1/0/2     Yes
Domain ID    : 2
Control VLAN  : Major 10   Sub 11
Hello Timer   : 1  sec  Fail Timer : 3  sec
Protected VLAN: Reference Instance 0 to 2, 4
 Ring  Ring   Node  Primary/Common          Secondary/Edge          Enable
 ID    Level  Mode  Port                  Port                  Status
--------------------------------------------------------------------------------
 1    0     T    GigabitEthernet1/0/3     GigabitEthernet1/0/4     Yes
 2    1     E    GigabitEthernet1/0/3     GigabitEthernet1/0/5     Yes
                GigabitEthernet1/0/4
```

Table 3-1 display rrpp brief command output description

Field	Description
Flags for Node Mode	RRPP node mode • M represents master node • T represents transit node • E represents edge node • A represents assistant edge node
RRPP Protocol Status	RRPP protocol status • Enable (globally enabled) • Disable (globally disabled)
Number of RRPP Domains	Number of RRPP domains configured
Domain ID	RRPP domain ID
Control VLAN	Control VLANs of the RRPP domain: Major and Sub
Protected VLAN	List of VLANs protected by the RRPP domain. MSTIs are displayed here. To get the VLANs corresponding to these MSTIs, use the **display stp region-configuration** command.
Hello Timer	Hello Timer value in seconds
Fail Timer	Fail Timer value in seconds
Ring ID	RRPP ring ID
Ring Level	RRPP ring level • 0 representing primary ring • 1 representing subring
Node Mode	Node mode
Primary/Common Port	• Primary port when the node mode is master node or transit node • Common port when the node mode is edge node or assistant edge node • "-" appears when the port is not configured on the ring or the board to which the port belongs does not start
Secondary/Edge Port	• Secondary port when the node mode is master node or transit node • Edge port when the node mode is edge node or assistant edge node • "-" appears when the port is not configured on the ring or the board to which the port belongs does not start
Enable Status	RRPP ring status • Yes indicates enabled • No indicates disabled

display rrpp ring-group

Syntax

display rrpp ring-group [*ring-group-id*]

View

Any view

Default Level

1: Monitor Level

Parameters

ring-group-id: RRPP ring group ID, in the range 1 to 8.

Description

Use the **display rrpp ring-group** command to display the RRPP ring group configuration. If no ring group ID is specified, the configuration of all ring groups is displayed. If an RRPP ring ID is specified, the configuration of the specified RRPP ring group on the current device is displayed. For an edge node RRPP ring group, the subring sending Edge-Hello packets is also displayed.

Related commands: **domain ring**.

Examples

Display the configuration of all RRPP ring groups.

```
<Sysname> display rrpp ring-group
Ring Group 1:
domain 1 ring 1 to 3, 5
domain 2 ring 1 to 3, 5
domain 1 ring 1 is the sending ring

Ring Group 2:
domain 1 ring 4, 6 to 7
domain 2 ring 4, 6 to 7
```

Table 3-2 display rrpp ring-group command output description

Field	Description
Ring Group 1	RRPP ring group 1.
domain 1 ring 1 to 3, 5	Subrings in the ring group, including rings 1, 2, 3, and 5 in RRPP domain 1.
domain 1 ring 1 is the sending ring	The sending ring of the ring group is ring 1 in RRPP domain 1.

display rrpp statistics

Syntax

display rrpp statistics domain *domain-id* [**ring** *ring-id*]

View

Any view

Default Level

1: Monitor level

Parameters

domain-id: RRPP domain ID, in the range 1 to 8.

ring-id: RRPP ring ID, in the range 1 to 64.

Description

Use the **display rrpp statistics** command to display RRPPDU statistics.

Note that:

- If an RRPP ring ID is specified, the RRPPDU statistics for the specified RRPP ring in the specified RRPP domain on the current device are displayed. If not, the RRPPDU statistics for all RRPP rings in the specified RRPP domain are displayed.
- If a certain port belongs to more than one ring, its RRPPDU statistics are collected and displayed by ring.
- When a ring transits from inactive status into active status, packet counting for the ring restarts.

Related commands: **reset rrpp statistics**.

Examples

Display the RRPPDU statistics for ring 1 in RRPP domain 1.

```
<Sysname> display rrpp statistics domain 1 ring 1
Ring ID      : 1
Ring Level   : 1
Node Mode    : Master
Active Status : Yes
Primary port  : GigabitEthernet1/0/1
 Packet          Link     Common    Complete   Edge     Major    Packet
 Direct Hello    Down     Flush FDB  Flush FDB  Hello    Fault    Total
--------------------------------------------------------------------------------
 Send   16424    0        0         1         0        0        16425
 Rcv    0        0        0         0         0        0        0
Secondary port: GigabitEthernet1/0/2
 Packet          Link     Common    Complete   Edge     Major    Packet
 Direct Hello    Down     Flush FDB  Flush FDB  Hello    Fault    Total
--------------------------------------------------------------------------------
 Send   0        0        0                   0        0        0
 Rcv    16378    0        0         1         0        0        16379
```

Display the RRPPDU statistics for all rings in RRPP domain 2.

```
<Sysname> display rrpp statistics domain 2
Ring ID      : 1
Ring Level   : 0
Node Mode    : Master
Active Status : Yes
Primary port  : GigabitEthernet1/0/3
 Packet          Link     Common    Complete   Edge     Major    Packet
 Direct Hello    Down     Flush FDB  Flush FDB  Hello    Fault    Total
--------------------------------------------------------------------------------
 Send   16924    0        0         1         0        0        16925
```

```
 Rcv    0        0        0         0         0        0        0
Secondary port: GigabitEthernet1/0/4
 Packet          Link     Common    Complete   Edge     Major    Packet
 Direct Hello    Down     Flush FDB  Flush FDB  Hello    Fault    Total
--------------------------------------------------------------------------------
 Send   0        0        0         0         0        0        0
 Rcv    16878    0        0         1         0        0        16879
Ring ID      : 2
Ring Level   : 1
Node Mode    : Edge
Active Status : No
Common port   : GigabitEthernet1/0/3
 Packet          Link     Common    Complete   Edge     Major    Packet
 Direct Hello    Down     Flush FDB  Flush FDB  Hello    Fault    Total
--------------------------------------------------------------------------------
 Send   0        0        0         0         0        0        0
 Rcv    0        0        0         0         0        0        0
Common port   : GigabitEthernet1/0/4
 Packet          Link     Common    Complete   Edge     Major    Packet
 Direct Hello    Down     Flush FDB  Flush FDB  Hello    Fault    Total
--------------------------------------------------------------------------------
 Send   0        0        0         0         0        0        0
 Rcv    0        0        0         0         0        0        0
Edge port    : GigabitEthernet1/0/5
 Packet          Link     Common    Complete   Edge     Major    Packet
 Direct Hello    Down     Flush FDB  Flush FDB  Hello    Fault    Total
--------------------------------------------------------------------------------
 Send   0        0        0         0         0        0        0
 Rcv    0        0        0         0         0        0        0
```

Table 3-3 display rrpp statistics command output description

Field	Description
Ring ID	RRPP ring ID
Ring Level	RRPP ring level: • 0 for primary ring • 1 for subring
Node Mode	Node mode: • Master node • Transit node • Edge node • Assistant edge node
Active Status	RRPP ring activation status: • Yes for active • No for inactive
Primary Port	The primary port field means the node mode is master node or transit node. “-“ appears when the port is not configured on the ring or the board to which the port belongs does not start, and in this case, no corresponding statistics appears.

Field	Description
Secondary Port	The secondary port field means the node mode is master node or transit node. “-” appears when the port is not configured on the ring or the board to which the port belongs does not start, and in this case, no corresponding statistics appears.
Common Port	The common port field means the node mode is edge node or assistant edge node. “-” appears when the port is not configured on the ring or the board to which the port belongs does not start, and in this case, no corresponding statistics appears.
Edge Port	The edge port field means the node mode is edge node or assistant edge node. “-” appears when the port is not configured on the ring or the board to which the port belongs does not start, and in this case, no corresponding statistics appears.
Packet Direct	Packet transmission direction on the port: Send or Rcv
Hello	Hello packet statistics received/sent on the port
Link-Down	Link-Down packet statistics received/sent on the port
Common Flush FDB	Common-Flush-FDB packet statistics received/sent on the port
Complete Flush FDB	Complete-Flush-FDB packet statistics received/sent on the port
Edge Hello	Edge-Hello packet statistics received/sent on the port
Major Fault	Major-Fault packet statistics received/sent on the port
Packet Total	Total number of packets received/sent on the port. Here only Hello, Link-Down, Common-Flush-FDB, Complete-Flush-FDB, Edge-Hello, and Major-Fault packets of RRPP are counted.

display rrpp verbose

Syntax

display rrpp verbose domain *domain-id* [**ring** *ring-id*]

View

Any view

Default Level

1: Monitor level

Parameters

domain-id: RRPP domain ID, in the range 1 to 8.

ring-id: RRPP ring ID, in the range 1 to 64.

Description

Use the **display rrpp verbose** command to display detailed RRPP information.

If you have specified an RRPP ring ID in the command, the detailed information of the specified ring in the specified RRPP domain appears. Otherwise, the detailed information of all the rings in the specified RRPP domain appears.

Examples

Display the detailed information of ring 1 in RRPP domain 1.

```
<Sysname> display rrpp verbose domain 1 ring 1
Domain ID    : 1
Control VLAN  : Major 5    Sub 6
Protected VLAN: Reference Instance 0 to 2, 4
Hello Timer   : 1  sec  Fail Timer : 3  sec
Ring ID      : 1
Ring Level    : 1
Node Mode     : Master
Ring State    : Complete
Enable Status : Yes    Active Status: Yes
Primary port  : GigabitEthernet1/0/1           Port status: UP
Secondary port: GigabitEthernet1/0/2           Port status: BLOCKED
```

Display the detailed information of all the rings in RRPP domain 2.

```
<Sysname> display rrpp verbose domain 2
Domain ID    : 2
Control VLAN  : Major 10    Sub 11
Protected VLAN: Reference Instance 3, 5 to 7
Hello Timer   : 1  sec  Fail Timer : 3  sec

Ring ID      : 1
Ring Level    : 0
Node Mode     : Master
Ring State    : Complete
Enable Status : Yes    Active Status: Yes
Primary port  : GigabitEthernet1/0/4           Port status: UP
Secondary port: GigabitEthernet1/0/5           Port status: BLOCKED

Ring ID      : 2
Ring Level    : 1
Node Mode     : Edge
Ring State    : -
Enable Status : No    Active Status: No
Common port   : GigabitEthernet1/0/4           Port status: -
              GigabitEthernet1/0/5           Port status: -
Edge port     : GigabitEthernet1/0/3           Port status: -
```

Table 3-4 display rrpp verbose command output description

Field	Description
Domain ID	RRPP domain ID
Control VLAN	Control VLANs of the RRPP domain: • Major: Represents the primary control VLAN • Sub: Represents the secondary control VLAN

Field	Description
Protected VLAN	List of VLANs protected by the RRPP domain. MSTIs are displayed here. To get the VLANs corresponding to these MSTIs, use the **display stp region-configuration** command.
Hello Timer	Hello Timer value in seconds
Fail Timer	Fail Timer value in seconds
Ring ID	RRPP ring ID
Ring Level	RRPP ring level: • 0 representing primary ring • 1 representing subring
Node Mode	Node mode: • Master node • Transit node • Edge node • Assistant edge node
Ring State	RRPP ring state. This field makes sense only when the node mode field is master node. • “Complete” appears when the ring is in health state; • “Failed” appears when the ring is in disconnect sate; • “–” appears in all the other cases.
Enable Status	RRPP ring enable status • Yes for enabled • No for disabled
Active Status	RRPP ring activation status. An RRPP ring can be active only when the RRPP protocol and the RRPP ring are both enabled. Therefore, you can also use this field to identify whether the RRPP protocol are enabled. Two statuses are available: • Yes for active • No for inactive
Primary Port	The primary port field means the node mode is master node or transit node. “-“ appears when the port is not configured on the ring or the board to which the port belongs does not start.
Secondary Port	The secondary port field means the node mode is master node or transit node. **-** appears when the port is not configured on the ring or the board to which the port belongs does not start.
Common Port	The common port field means the node mode is edge node or assistant edge node. “-“ appears when the port is not configured on the ring or the board to which the port belongs does not start.
Edge Port	The edge port field means the node mode is edge node or assistant edge node. “-“ appears when the port is not configured on the ring or the board to which the port belongs does not start.
Port status	Port status includes down, up and blocked; “-“ appears in one of the following cases: • the ring is inactive • the port is not configured on the ring • the board to which the port belongs does not start

domain ring

Syntax

domain *domain-id* **ring** *ring-id-list*

undo domain *domain-id* [**ring** *ring-id-list*]

View

RRPP ring group view

Default Level

2: System level

Parameters

domain-id: RRPP domain ID, in the range of 1 to 8.

ring-id-list: RRPP subring ID list expressed in the format of *ring-id-list*={ *ring-id* [**to** *ring-id*] }&<1-10>, where the *ring-id* argument is an RRPP subring ID in the range of 1 to 64 and &<1-10> indicates that you can input up to ten RRPP ring ID ranges.

Description

Use the **domain ring** command to configure subrings for an RRPP ring group.

Use the **undo domain ring** command to remove the specified subring(s) from an RRPP ring group. If no subring ID list is specified, all subrings in the ring group are removed in the specified domain.

Note that:

- A subring can be assigned to only one ring group.
- A device must be of the same type, an edge node or an assistant-edge node, in the subrings in a ring group.
- The subrings in a ring group must have the same link in the primary ring. Otherwise, the ring group cannot function properly.
- An edge node ring group and its corresponding assistant-edge node ring group must be the same in configurations and activation status.

Moreover, you must follow these guidelines when configuring an RRPP ring group on the edge node and the assistant-edge node:

- When assigning an active ring to a ring group, do that on the assistant-edge node first and then on the edge node.
- To remove an active ring from a ring group, do that on the edge node first and then on the assistant-edge node.
- To remove the whole ring group, do that on the edge node first and then on the assistant-edge node.
- When activating rings in a ring group, do that on the assistant-edge node first and then on the edge node.
- When deactivating rings in a ring group, do that on the edge node first and then on the assistant-edge node.

Failure to follow these guidelines may cause the failure of assistant-edge node to receive Edge-Hello packets and thus mistakenly considering the primary ring as failed.

Related commands: **rrpp ring-group**, **display rrpp ring-group**.

Examples

Configure subrings for RRPP ring group 1.

```
<Sysname> system-view
[Sysname] rrpp ring-group 1
[Sysname-rrpp-ring-group1] domain 1 ring 1 to 3 5
[Sysname-rrpp-ring-group1] domain 2 ring 1 to 3 5
```

protected-vlan

Syntax

protected-vlan reference-instance *instance-id-list*

undo protected-vlan [**reference-instance** *instance-id-list*]

View

RRPP domain view

Default Level

2: System level

Parameters

reference-instance *instance-id-list*: Specifies the MSTIs to be referenced. The range of the *instance-id-list* argument is as specified in the command configuring MSTIs.

Description

Use the **protected-vlan** command to configure the protected VLANs for the RRPP domain. The protected VLANs are specified by the MSTIs.

Use the **undo protected-vlan** command to remove the specified protected VLANs of the RRPP domain. If no MSTI is specified, all protected VLANs of the RRPP domain are removed.

By default, no protected VLAN is specified for an RRPP domain.

Note that:

- To be compatible with old-version RRPP, which does not support protected VLAN configuration, an RRPP domain protects all VLANs on a device started with an old-version configuration file.
- You can use the **display stp region-configuration** command to check the VLANs corresponding to the specified MSTIs.
- Before configuring rings for an RRPP domain, you can delete or modify the protected VLANs configured for the RRPP domain; after configuring rings for an RRPP domain, you can delete or modify the protected VLANs configured for the RRPP domain, however, you cannot delete all the protected VLANs configured for the domain.
- When the VLAN-to-MSTI mappings change, the protected VLANs of an RRPP domain also changes according to the MSTIs configured for the domain.

Related commands: **rrpp domain**, **display stp region-configuration** in *MSTP Configuration Commands* in the *Access Volume*.

Examples

Configure VLANs mapped to MSTI 2 and MSTI 3 as the protected VLANs of RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protected-vlan reference-instance 2 to 3
```

reset rrpp statistics

Syntax

reset rrpp statistics domain *domain-id* [**ring** *ring-id*]

View

User view

Default Level

1: Monitor level

Parameters

domain-id: RRPP domain ID, in the range 1 to 8.

ring-id: RRPP ring ID, in the range 1 to 64.

Description

Use the **reset rrpp statistics** command to clear RRPPDU statistics.

If you have specified an RRPP ring ID in the command, RRPPDU statistics of the specified RRPP ring in the specified RRPP domain on the current device are cleared. Otherwise, RRPPDU statistics of all RRPP rings in the specified RRPP domain are cleared.

Related commands: **display rrpp statistics**.

Examples

Clear the RRPPDU statistics of ring 10 in RRPP domain 10.

```
<Sysname> reset rrpp statistics domain 1 ring 10
```

ring

Syntax

ring *ring-id* **node-mode** { { **master** | **transit** } [**primary-port** *interface-type interface-number*] [**secondary-port** *interface-type interface-number*] **level** *level-value* | { **edge** | **assistant-edge** } [**edge-port** *interface-type interface-number*] }

undo ring *ring-id*

View

RRPP domain view

Default Level

2: System level

Parameters

ring-id: RRPP ring ID, in the range 1 to 64.

master: Specifies the device as the master node of the RRPP ring.

transit: Specifies the device as the transit node of the RRPP ring.

primary-port: Specifies the port as a primary port.

interface-type interface-number: Specifies a port by its type and number. The port can be a Layer-2 GE port, Layer-2 XGE port, or Layer-2 aggregate port, and cannot be member ports of any aggregation group, or smart link group.

secondary-port: Specifies the port as a secondary port.

level-value: RRPP ring level, with 0 representing primary ring and 1 representing subring.

edge: Specifies the device as the edge node of the RRPP ring.

assistant-edge: Specifies the device as the assistant edge node of the RRPP ring.

edge-port: Specifies the edge port for the node.

Description

Use the **ring** command to configure the node mode of the device, the role of the specified RRPP port, and the level of the RRPP ring.

Use the **undo ring** command to remove the configuration.

Note that:

- Before configuring rings for an RRPP domain, configure the control VLANs and protected VLANs for the RRPP domain first.
- The ID of an RRPP ring in a domain must be unique.
- The maximum number of rings that can be configured on a device in all RRPP domains is 16.
- If a device resides on multiple RRPP rings in an RRPP domain, only one primary ring exists within these rings. The device plays a role of either edge node or assistant edge node on other subrings.
- When an RRPP is enabled, you cannot configure its RRPP ports.
- When configuring the edge node and the assistant-edge node, you must first configure the primary ring, and then the subrings.
- The node mode, RRPP port role, and ring level settings of an RRPP ring cannot be modified once they are configured. To modify the settings, you must first remove the present settings.
- You must remove all subring configurations before deleting the primary ring configuration of the edge node or the assistant-edge node. However, an active RRPP ring cannot be deleted.

Related command: **ring enable**.

Examples

Specify the device as the master node of primary ring 10 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

Specify the device as the transit node of primary ring 10 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
```

Specify the device as the master node of subring 20 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 20 node-mode master primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1
```

Specify the device as the transit node of primary ring 20 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 20 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 1
```

Specify the device as the transit node of primary ring 10 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Then, specify the device as the edge node of subring 20 in RRPP domain 1, GigabitEthernet 1/0/3 as the edge port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[Sysname-rrpp-domain1] ring 20 node-mode edge edge-port gigabitethernet 1/0/3
```

Specify the device as the transit node of primary ring 10 in RRPP domain 1, GigabitEthernet 1/0/1 as the primary port and GigabitEthernet 1/0/2 as the secondary port. Then, specify the device as the assistant edge node of subring 20 in RRPP domain 1, GigabitEthernet 1/0/3 as the edge port.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode transit primary-port gigabitethernet 1/0/1 secondary-port gigabitethernet 1/0/2 level 0
[Sysname-rrpp-domain1] ring 20 node-mode assistant-edge edge-port gigabitethernet 1/0/3
```

ring enable

Syntax

ring *ring-id* **enable**

undo ring *ring-id* **enable**

View

RRPP domain view

Default Level

2: System level

Parameters

ring-id: RRPP ring ID, in the range 1 to 64.

Description

Use the **ring enable** command to enable the RRPP ring.

Use the **undo ring enable** command to disable the RRPP ring.

By default, the RRPP ring is disabled.

Note that:

- To enable subrings, you must first enable the primary ring before enabling subrings.
- You must first disable all the subrings in the RRPP domain and then disable the primary ring.
- To activate the RRPP domain, enable the RRPP protocol and the RRPP rings for the RRPP domain.

Related commands: **rrpp enable**.

Examples

Enable RRPP ring 10 in RRPP domain 1.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] control-vlan 100
[Sysname-rrpp-domain1] protect-vlan reference-instance 0 1 2
[Sysname-rrpp-domain1] ring 10 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
[Sysname-rrpp-domain1] ring 10 enable
```

rrpp domain

Syntax

rrpp domain *domain-id*

undo rrpp domain *domain-id*

View

System view

Default Level

2: System level

Parameters

domain-id: RRPP domain ID, in the range 1 to 8.

Description

Use the **rrpp domain** command to create an RRPP domain and enter its view.

Use the **undo rrpp domain** command to remove an RRPP domain.

Note that:

- When you delete an RRPP domain, the control VLANs and protected VLANs of it are deleted at the same time.
- To delete an RRPP domain successfully, be sure that it has no RRPP rings.

Related commands: **control-vlan**, **protected-vlan**.

Examples

Create RRPP domain 1, and enter RRPP domain 1 view.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1]
```

rrpp enable

Syntax

rrpp enable

undo rrpp enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **rrpp enable** command to enable RRPP protocol.

Use the **undo rrpp enable** command to disable RRPP protocol.

By default, RRPP protocol is disabled.

To activate the RRPP domain, enable the RRPP protocol and the RRPP rings for the RRPP domain.

Related commands: **ring enable**.

Examples

Enable the RRPP protocol.

```
<Sysname> system-view
[Sysname] rrpp enable
```

rrpp ring-group

Syntax

rrpp ring-group *ring-group-id*

undo rrpp ring-group *ring-group-id*

View

System view

Default Level

2: System level

Parameters

ring-group-id: RRPP ring group ID, in the range 1 to 8.

Description

Use the **rrpp ring-group** command to create an RRPP ring group and enter RRPP ring group view.

Use the **undo rrpp ring-group** command to delete an RRPP ring group.

Note that:

- RRPP configured with ring groups cannot interoperate with RRPP that does not support ring group configuration.
- When removing a ring group, do that on the edge node first and then on the assistant-edge node. If you fail to follow the order, the assistant-edge node may fail to receive Edge-Hello packets and thus mistakenly considers that the primary ring has failed.
- After a ring group is removed, all subrings in the ring group do not belong to any ring group.

Related commands: **domain ring**, **display rrpp ring-group**.

Examples

Create RRPP ring group 1 and enter its view.

```
<Sysname> system-view
[Sysname] rrpp ring-group 1
[Sysname-rrpp-ring-group1]
```

timer

Syntax

timer hello-timer *hello-value* **fail-timer** *fail-value*

undo timer

View

RRPP domain view

Default Level

2: System level

Parameters

hello-value: Hello timer value, in the range 1 to 10 seconds.

fail-value: Fail timer value, in the range 3 to 30 seconds.

Description

Use the **timer** command to configure the Hello timer value and the Fail timer value for the RRPP domain.

Use the **undo timer** command to restore it to the default value.

By default, the Hello timer value is 1 second and the Fail timer value is 3 seconds.

Note that the Fail timer value must be greater than or equal to three times of the Hello timer value.

Examples

Set the Hello timer value to 2 seconds and the Fail timer value to 7 seconds.

```
<Sysname> system-view
[Sysname] rrpp domain 1
[Sysname-rrpp-domain1] timer hello-timer 2 fail-timer 7
```

4 DLDP Configuration Commands

DLDP Configuration Commands

display dldp

Syntax

display dldp [*interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Port type and port number.

Description

Use the **display dldp** command to display the DLDP configuration of a port.

If you do not provide the *interface-type* or *interface-number* arguments, this command displays the DLDP configuration of all the DLDP-enabled ports.

Examples

Display the DLDP configuration of all the DLDP-enabled ports.

```
<Sysname> display dldp
 DLDP global status : enable
 DLDP interval : 5s
 DLDP work-mode : enhance
 DLDP authentication-mode : simple, password is 123
 DLDP unidirectional-shutdown : auto
 DLDP delaydown-timer : 2s
 The number of enabled ports is 2.

Interface GigabitEthernet1/0/50
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
   Neighbor mac address : 0000-0000-0100
   Neighbor port index : 79
   Neighbor state : two way
   Neighbor aged time : 13
```

```
Interface GigabitEthernet1/0/51
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
   Neighbor mac address : 0000-0000-1100
   Neighbor port index : 81
   Neighbor state : two way
   Neighbor aged time : 12
```

Display the DLDP configuration of GigabitEthernet 1/0/50.

```
<Sysname> display dldp gigabitethernet 1/0/50
Interface GigabitEthernet1/0/50
 DLDP port state : advertisement
 DLDP link state : up
 The neighbor number of the port is 1.
   Neighbor mac address : 0000-0000-0100
   Neighbor port index : 79
   Neighbor state : two way
   Neighbor aged time : 13
```

Table 4-1 display dldp command output description

Field	Description
DLDP global status	Global DLDP state (**enable** or **disable**)
DLDP interval	Interval for sending Advertisement packets (in seconds)
DLDP work-mode	DLDP mode (**enhance** or **normal**)
DLDP authentication-mode	DLDP authentication mode (**none**, **simple**, or **md5**)
password	Password for DLDP authentication
DLDP unidirectional-shutdown	Port shutdown mode (**auto** or **manual**)
DLDP delaydown-timer	Setting of the DelayDown timer
The number of enabled ports	Number of the DLDP-enabled ports
Interface	Index of a DLDP-enabled port
DLDP port state	DLDP state on a port (**initial**, **inactive**, **active**, **advertisement**, **probe**, **disable**, or **delaydown**)
DLDP link state	Port state (**up** or **down**)
The neighbor number of the port	Number of the neighbors of a port
Neighbor mac address	MAC address of a neighbor
Neighbor port index	Neighbor port index
Neighbor state	Neighbor state (**unknown**, **one way**, or **two way**)
Neighbor aged time	Neighbor aging time

display dldp statistics

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Port type and port number.

Description

Use the **display dldp statistics** command to display the statistics on the DLDP packets passing through a port.

If you do not provide the *interface-type* or *interface-number* argument, this command displays the statistics on the DLDP packets passing through all the DLDP-enabled ports.

Examples

Display the statistics on the DLDP packets passing through all the DLDP-enabled ports.

```
<Sysname> display dldp statistics
Interface GigabitEthernet1/0/50
 Packets sent : 6
 Packets received : 5
 Invalid packets received : 2
 Loop packets received : 0
 Authentication failed packets received : 0
 Valid packets received : 3

Interface GigabitEthernet1/0/51
 Packets sent : 7
 Packets received : 7
 Invalid packets received : 3
 Loop packets received : 0
 Authentication failed packets received : 0
 Valid packets received : 4
```

Display the statistics on the DLDP packets passing through GigabitEthernet 1/0/50.

```
<Sysname> display dldp statistics gigabitethernet 1/0/50
Interface GigabitEthernet1/0/50
 Packets sent : 6
 Packets received : 5
 Invalid packets received : 2
 Loop packets received : 0
 Authentication failed packets received : 0
```

```
Valid packets received : 3
```

Table 4-2 display dldp statistics command output description

Field	Description
Interface	Port index
Packets sent	Total number of DLDP packets sent
Packets received	Total number of DLDP packets received
Invalid packets received	Number of the invalid packets received
Loop packets received	Number of the loopback packets received
Authentication failed packets received	Number of the received packets that failed to pass the authentication
Valid packets received	Number of the valid packets received

dldp authentication-mode

Syntax

dldp authentication-mode { **md5** *md5-password* | **none** | **simple** *simple-password* }

undo dldp authentication-mode

View

System view

Default Level

2: System level

Parameters

md5 *md5-password*: Specifies to perform MD5 authentication and sets the password. The *md5-password* argument is the password, a string of 1 to 16 characters or a 24-bit string. The former indicates a plain text password and the latter indicates a cipher text password. Note that this argument is case-sensitive.

None: Specifies not to perform authentication.

simple *simple-password*: Specifies to perform plain text authentication and sets the password. The *simple-password* argument is the password, a case-sensitive string of 1 to 16 characters.

Description

Use the **dldp authentication-mode** command to configure DLDP authentication.

Use the **undo dldp authentication-mode** command to restore the default.

By default, DLDP authentication is not performed.

To enable DLDP to operate properly, make sure the DLDP authentication modes and the passwords of the both sides of a link are the same.

Examples

Configure to perform plain text authentication, setting the password as **abc** (assuming that Device A and Device B are connected by the DLDP link).

- Configuration on Device A

```
<DeviceA> system-view
[DeviceA] dldp authentication-mode simple abc
```

- Configuration on Device B

```
<DeviceB> system-view
[DeviceB] dldp authentication-mode simple abc
```

dldp delaydown-timer

Syntax

dldp delaydown-timer *time*

undo dldp delaydown-timer

View

System view

Default Level

2: System level

Parameters

Time: Setting of the DelayDown timer, in the range 1 to 5 (in seconds).

Description

Use the **dldp delaydown-timer** command to set the DelayDown timer.

Use the **undo dldp delaydown-timer** command to restore the default.

By default, the setting of the DelayDown timer is 1 second.

Note that the DelayDown timer configured using this command applies to all DLDP-enabled ports.

Examples

Set the DelayDown timer to 2 seconds.

```
<Sysname> system-view
[Sysname] dldp delaydown-timer 2
```

dldp enable

Syntax

dldp enable

undo dldp enable

View

System view, Ethernet port view, port group view

Default Level

2: System level

Parameters

None

Description

Use the **dldp enable** command to enable DLDP.

Use the **undo dldp enable** command to disable DLDP.

By default, DLDP is disabled both globally and on each port.

Note that:

- When executed in system view, these two commands enables/disables DLDP globally; when executed in Ethernet port view, these two commands enables/disables DLDP on the current port; when executed in port group view, these two commands enables/disables DLDP on all the ports in the port group.
- These two commands are applicable to Layer 2 Ethernet ports, including optical ports and electrical ports.
- DLDP can take effect only when it is enabled both globally and on a port.

Examples

Enable DLDP globally, and then enable DLDP on GigabitEthernet 1/0/50.

```
<Sysname> system-view
[Sysname] dldp enable
[Sysname] interface gigabitethernet 1/0/50
[Sysname-GigabitEthernet1/0/50] dldp enable
```

Enable DLDP globally, and then enable DLDP for all the ports in port group 1.

```
<Sysname> system-view
[Sysname] dldp enable
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet 1/0/50 to gigabitethernet 1/0/52
[Sysname-port-group-manual-1] dldp enable
```

dldp interval

Syntax

dldp interval *time*

undo dldp interval

View

System view

Default Level

2: System level

Parameters

time: Interval for sending Advertisement packets, in the range 1 to 100 (in seconds).

Description

Use the **dldp interval** command to set the interval for sending Advertisement packets.

Use the **undo dldp interval** command to restore the default.

By default, the interval for sending Advertisement packets is 5 seconds.

Note that:

- These two commands apply to all DLDP-enabled ports.
- Set the interval for sending Advertisement packets to a value not longer than one-third of the STP convergence time. If the interval is too long, STP loops may occur before unidirectional links are torn down; if the interval is too short, network traffic may increase in vain due to excessive Advertisement packets. You are recommended to use the default value.

Examples

Set the interval for sending Advertisement packets to 20 seconds.

```
<Sysname> system-view
[Sysname] dldp interval 20
```

dldp reset

Syntax

dldp reset

View

System view, Ethernet port view, port group view

Default Level

2: System level

Parameters

None

Description

Use the **dldp reset** command to reset DLDP state for ports shut down by DLDP to enable them to perform unidirectional link detect.

When executed in system view, this command applies to all the ports shut down by DLDP; when executed in Ethernet port view, this command applies to the current port; when executed in port group view, this command applies to all the ports in the port group shut down by DLDP.

Related commands: **dldp enable**, **dldp unidirectional-shutdown**.

Examples

Reset DLDP state for all the ports shut down by DLDP.

```
<Sysname> system-view
[Sysname] dldp reset
```

Reset DLDP state for GigabitEthernet 1/0/50 (assuming that GigabitEthernet 1/0/50 is shut down by DLDP).

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/50
[Sysname-GigabitEthernet1/0/50] dldp reset
```

Reset DLDP state for all the ports in port group 1 shut down by DLDP.

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member gigabitethernet 1/0/50 to gigabitethernet 1/0/52
[Sysname-port-group-manual-1] dldp reset
```

dldp unidirectional-shutdown

Syntax

dldp unidirectional-shutdown { **auto** | **manual** }

undo dldp unidirectional-shutdown

View

System view

Default Level

2: System level

Parameters

auto: Sets the port shutdown mode as auto mode, where, when a unidirectional link is detected, the port involved is shut down by DLDP.

manual: Sets the port shutdown mode as manual mode, where, when a unidirectional link is detected, DLDP prompts you to shut down the involved port instead of doing so automatically.

Description

Use the **dldp unidirectional-shutdown** command to set the port shutdown mode.

Use the **undo dldp unidirectional-shutdown** command to restore the default.

By default, the port shutdown mode is auto mode.

Related commands: **dldp work-mode**.

Examples

Set the port shutdown mode as auto mode.

```
<Sysname> system-view
[Sysname] dldp unidirectional-shutdown auto
```

dldp work-mode

Syntax

dldp work-mode { **enhance** | **normal** }

undo dldp work-mode

View

System view

Default Level

2: System level

Parameters

enhance: Specifies the enhanced DLDP mode.

normal: Specifies the normal DLDP mode.

Description

Use the **dldp work-mode** command to set the DLDP mode.

Use the **undo dldp work-mode** command to restore the default DLDP mode.

By default, a device operates in normal DLDP mode.

Examples

Configure the device to operate in enhanced DLDP mode.

```
<Sysname> system-view
[Sysname] dldp work-mode enhance
```

reset dldp statistics

Syntax

reset dldp statistics [*interface-type interface-number*]

View

User view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Port type and port number.

Description

Use the **reset dldp statistics** command to clear the statistics on DLDP packets passing through a port.

If you do not provide the *interface-type* or *interface-number* argument, this command clears the statistics on the DLDP packets passing through all the DLDP-enabled ports.

Examples

Clear the statistics on the DLDP packets passing through all the DLDP-enabled ports.

```
<Sysname> reset dldp statistics
```

5 Ethernet OAM Configuration Commands

OAM Configuration Commands

display oam

Syntax

display oam { **local** | **remote** } [**interface** *interface-type interface-number*]

View

Any view

Default Level

2: System level

Parameters

local: Displays the Ethernet OAM connection information of the local end.

remote: Displays the Ethernet OAM connection information of the remote end.

interface *interface-type interface-number*: Specify a port by its type and number.

Description

Use the **display oam** command to display the information about an Ethernet OAM connection, including connection status, information contained in Ethernet OAM packet header, and Ethernet OAM packet statistics.

If you do not specify the **interface** keyword, this command displays the information about all the Ethernet OAM connections.

Related commands: **reset oam**.

Examples

Display the information about the Ethernet OAM connection established on the local port GigabitEthernet 1/0/1.

```
<Sysname> display oam local interface gigabitethernet 1/0/1
Port       : GigabitEthernet1/0/1
Link Status : Up
EnableStatus            : Enable
Local_oam_mode          : Active     Local_pdu            : ANY
Local_mux_action        : FWD        Local_par_action      : FWD

OAMLocalFlagsField :
--------------------------------------------------------------------------
Link Fault              : 0          Dying Gasp           : 0
Critical Event          : 0          Local Evaluating      : COMPLETE
```

```
Remote Evaluating       : COMPLETE

Packets statistic :
Packets                     Send                Receive
--------------------------------------------------------------------------
OAMPDU                     645                 648
OAMInformation              645                 648
OAMEventNotification         0                   --
OAMUniqueEventNotification    --                  0
OAMDuplicateEventNotification  --                  0
```

Table 5-1 display oam local command output description

Field	Description
Port	Port index
Link Status	Link status
EnableStatus	Ethernet OAM state (enabled or disabled)
Local_oam_mode	Local Ethernet OAM mode, which can be: • Active, indicating the port operates in the active Ethernet OAM mode • Passive, indicating the port operates in the passive Ethernet OAM mode
Local_pdu	The way in which the local end processes Ethernet OAMPDUs: • RX_INFO, indicating the port only receives Information OAMPDUs and does not send any Ethernet OAMPDUs. • LF_INFO, indicating the port only sends the Information OAMPDUs without Information TLV triplets and with their link error flag bits being set. • INFO, indicating the port sends and receives only Information OAMPDUs. • ANY, indicating the port sends and receives Ethernet OAMPDUs of any type.
Local_mux_action	Working mode of the local transmitter, which can be: • FWD, indicating the port can send any packets. • DISCARD, indicating the port only sends Ethernet OAMPDUs.
Local_par_action	Working mode of the local receiver, which can be: • FWD, indicating the port can receive any packets. • DISCARD, indicating the port only receives Ethernet OAMPDUs. • LB, indicating Ethernet OAM loopback testing is enabled on the port. In this case, all the packets other than Ethernet OAMPDUs received are returned to their sources along the ways they come.
OAMLocalFlagsField	Local flags inserted in the local flag fields of the Ethernet OAMPDUs sent.
Link Fault	Indicates whether an Ethernet OAM link error is present: 0 for no and 1 for yes.
Dying Gasp	Indicates whether a fatal error is present: 0 for no and 1 for yes.
Critical Event	Indicates whether a critical error is present: 0 for no and 1 for yes.

Field	Description
Local Evaluating	Indicates whether the local-to-remote configuration negotiation is complete: • COMPLETE for completed • REVERSED for uncompleted
Remote Evaluating	Indicates whether the remote-to-local configuration negotiation is complete: • COMPLETE for completed • REVERSED for uncompleted
Packets statistic	Statistics about Ethernet OAMPDUs sent and received
OAMPDU	Total number of the Ethernet OAMPDUs sent and received
OAMInformation	Number of the Information OAMPDUs sent and received
OAMEventNotification	Number of the Event notification OAMPDUs sent and received
OAMUniqueEventNotification	Number of the unduplicated Event notification OAMPDUs sent or received uniquely.
OAMDuplicateEventNotification	Number of the duplicate Event notification OAMPDUs sent or received.

Display the Ethernet OAM information of the peer port GigabitEthernet 1/0/1.

```
<Sysname> display oam remote interface gigabitethernet 1/0/1
Port       : GigabitEthernet1/0/1
Link Status : Up
Information of the latest received OAM packet:
OAMRemoteMACAddress      : 00e0-fd73-6502
OAMRemotePDUConfiguration : 1500

OAMRemoteState :
------------------------------------------------------------------------------
Remote_mux_action        : FWD        Remote_par_action     : FWD

OAMRemoteConfiguration :
------------------------------------------------------------------------------
OAM Mode               : Active     Unidirectional Support : YES
Loopback Support         : YES        Link Events           : YES
Variable Retrieval       : NO

OAMRemoteFlagsField :
------------------------------------------------------------------------------
Link Fault             : 0          Dying Gasp            : 0
Critical Event           : 0          Local Evaluating      : COMPLETE
Remote Evaluating        : COMPLETE
```

Table 5-2 display oam remote port command output description

Field	Description
Port	Port index
Link Status	Link status
Information of the latest received OAM packet	Information about the latest received Ethernet OAMPDU
OAMRemoteMACAddress	MAC address of the Ethernet OAM peer
OAMRemotePDUConfiguration	Maximum Ethernet OAMPDU size allowed
OAMRemoteState	State of the Ethernet OAM peer
Remote_mux_action	Peer sending mode. Refer to Table 5-1 for more.
Remote_par_action	Peer receiving mode. Refer to Table 5-1 for more.
OAMRemoteConfiguration	Configuration of the peer Ethernet OAM entity
OAM Mode	Ethernet OAM mode
Unidirectional Support	Indicates whether unidirectional transmission is supported (YES or NO)
Loopback Support	Indicates whether Ethernet OAM loopback testing is supported (YES or NO)
Link Events	Indicates whether Ethernet OAM link error events are supported (YES or NO)
Variable Retrieval	Indicates whether MIB variable retrieval is supported (YES or NO)
OAMRemoteFlagsField	Values of the peer Ethernet OAM flag fields in OAM packets
Link Fault	Indicates whether a link fault is present: 0 for no and 1 for yes.
Dying Gasp	Indicate whether a fatal fault is present: 0 for no and 1 for yes.
Critical Event	Indicate whether a critical fault is present: 0 for no and 1 for yes.
Local Evaluating	Indicates whether the local-to-remote configuration negotiation is complete: • COMPLETE for completed • REVERSED for uncompleted
Remote Evaluating	Indicates whether the remote-to-local configuration negotiation is complete: • COMPLETE for completed • REVERSED for uncompleted

display oam configuration

Syntax

display oam configuration

View

Any view

Default Level

2: System level

Parameters

None

Description

Use the **display oam configuration** command to display global Ethernet OAM configuration, including the periods and thresholds for Ethernet OAM link error event detection.

Related commands: **oam errored-symbol period**, **oam errored-symbol threshold**, **oam errored-frame period**, **oam errored-frame threshold**, **oam errored-frame-period period**, **oam errored-frame-period threshold**, **oam errored-frame-seconds period**, **oam errored-frame-seconds threshold**.

Examples

Display global Ethernet OAM configuration.

```
<Sysname> display oam configuration
Configuration of the link event window/threshold :
--------------------------------------------------------------------------
Errored-symbol Event period(in seconds)         :    1
Errored-symbol Event threshold                 :    1
Errored-frame Event period(in seconds)          :    1
Errored-frame Event threshold                  :    1
Errored-frame-period Event period(in ms)        :    1000
Errored-frame-period Event threshold           :    1
Errored-frame-seconds Event period(in seconds)   :    60
Errored-frame-seconds Event threshold          :    1
```

Table 5-3 display oam configuration command output description

Field	Description
Configuration of the link event window/threshold	Detection intervals and triggering thresholds configured for link events
Errored-symbol Event period (in seconds)	Errored symbol detection interval, which defaults to one second.
Errored-symbol Event threshold	Errored symbol event triggering threshold, which defaults to 1.
Errored-frame Event period (in seconds)	Errored frame detection interval, which defaults to one second.
Errored-frame Event threshold	Errored frame event triggering threshold, which defaults to 1.
Errored-frame-period Event period (in ms)	Errored frame period detection interval, which defaults to 1000 milliseconds.
Errored-frame-period Event threshold	Errored frame period event triggering threshold, which defaults to 1.
Errored-frame-seconds Event period (in seconds)	Errored frame seconds detection interval, which defaults to 60 seconds.

Field	Description
Errored-frame-seconds Event threshold	Errored frame seconds event triggering threshold, which defaults to 1.

display oam critical-event

Syntax

display oam critical-event [**interface** *interface-type interface-number*]

View

Any view

Default Level

2: System level

Parameters

interface *interface-type interface-number*: Specify a port by its type and number.

Description

Use the **display oam critical-event** command to display the statistics on critical Ethernet OAM link events occurred on a port.

If you do not specify the **interface** keyword, this command displays the statistics on the critical Ethernet OAM link events occurred on all the ports of the switch.

Examples

Display the statistics on critical Ethernet OAM link events occurred on all the ports.

```
<Sysname> display oam critical-event
Port       : GigabitEthernet1/0/1
Link Status : Up
Event statistic :
--------------------------------------------------------------------------
Link Fault    :0    Dying Gasp    : 0    Critical Event    : 0
```

Table 5-4 display oam critical-event command output description

Field	Description
Port	Port index
Link Status	Link status
Event statistic	Statistics on critical Ethernet OAM link events
Link Fault	Indicates whether a link fault is present: 0 for no and 1 for yes.
Dying Gasp	Indicate whether a fatal fault is present: 0 for no and 1 for yes.
Critical Event	Indicate whether a critical fault is present: 0 for no and 1 for yes.

display oam link-event

Syntax

display oam link-event { **local** | **remote** } [**interface** *interface-type interface-number*]

View

Any view

Default Level

2: System level

Parameters

local: Displays the statistics on the local Ethernet OAM link error events.

remote: Displays the statistics on the peer Ethernet OAM link error events.

interface *interface-type interface-number*: Specify a port by its type and number.

Description

Use the **display oam link-event** command to display the statistics on Ethernet OAM link error events occurred on a local port or a peer port. Ethernet OAM link error events include errored symbol events, errored frame events, errored frame period events, and errored frame seconds events.

If you do not specify the **interface** keyword, this command displays the statistics on the Ethernet OAM link error events occurred on all the local/peer ports.

Related commands: **display oam configuration**, **reset oam**.

Examples

Display the statistics on Ethernet OAM link error events occurred on all the local ports.

```
<Sysname> display oam link-event local
Port       : GigabitEthernet1/0/1
Link Status : Up

OAMLocalErrFrameEvent : (ms = milliseconds)
------------------------------------------------------------------------
Event Time Stamp        : 3539       Errored Frame Window  : 10(100ms)
Errored Frame Threshold   : 5         Errored Frame        : 1488111
Error Running Total      : 260908758   Event Running Total   : 307

OAMLocalErrFramePeriodEvent :
------------------------------------------------------------------------
Event Time Stamp        : 3539       Errored Frame Window  : 976500
Errored Frame Threshold   : 1         Errored Frame        : 1042054
Error Running Total      : 260909151   Event Running Total   : 471

OAMLocalErrFrameSecsSummaryEvent : (ms = milliseconds)
------------------------------------------------------------------------
Event Time Stamp : 3389
Errored Frame Second Summary Window    : 600(100ms)
```

```
Errored Frame Second Summary Threshold  : 1
Errored Frame Second Summary          : 60
Error Running Total      : 292       Event Running Total   : 5
```

Table 5-5 display oam link-event local command output description

Field	Description
Port	Port index
Link Status	Link status
OAMLocalErrFrameEvent	Information about local errored frame events. • Event Time Stamp: time when an errored frame event occurred (in 100 milliseconds). • Errored Frame Window: Error frame detection interval (in 100 milliseconds). • Errored Frame Threshold: error threshold that triggers an errored frame event. • Errored Frame: the number of detected error frames over the specific detection interval. • Error Running Total: the total number of error frames. • Event Running Total: the total number of errored frame events that have occurred.
OAMLocalErrFramePeriodEvent	Information about local errored frame period events: • Event Time Stamp: time when an errored frame event occurred (in 100 milliseconds). • Errored Frame Window: maximum number of 64-byte frames that can be transmitted through an Ethernet port over the configured error frame period detection interval. See **oam errored-frame-period period** command for more information. • Errored Frame Threshold: error threshold that triggers an error frame period event. • Errored Frame: the number of detected error frames over a detection interval. • Error Running Total: the total number of error frames that have detected. • Event Running Total: the total number of error frame period events.
OAMLocalErrFrameSecsSummaryEvent : (ms = milliseconds)	Information about local errored frame seconds events: • Event Time Stamp: time when an error frame seconds event occurred (in terms of 100 milliseconds). • Errored Frame Second Summary Window: error frame second detection interval (in 100 milliseconds). • Errored Frame Second Summary Threshold: error threshold that triggers an error frame seconds event. • Errored Frame Second Summary: the number of detected error frame seconds over a detection interval. • Error Running Total: the total number of error frame seconds. • Event Running Total: the total number of error frame seconds events that have occurred.

Display Ethernet OAM link event statistics of the remote ends of all the ports.

```
<Sysname> display oam link-event remote
Port : GigabitEthernet1/0/1
Link Status :Up
OAMRemoteErrFrameEvent : (ms = milliseconds)
```

```
------------------------------------------------------------------
Event Time Stamp        : 5789       Errored Frame Window   : 10(100ms)
Errored Frame Threshold   : 1         Errored Frame        : 3
Error Running Total      : 35        Event Running Total   : 17
```

Table 5-6 display oam link-event remote command output description

Field	Description
Port	Port index
Link Status	Link status
OAMLocalErrFrameEvent	Information about remote errored frame events. • Event Time Stamp: Time when an errored frame event occurred (in 100 milliseconds). • Errored Frame Window: Error frame detection interval (in 100 milliseconds). • Errored Frame Threshold: Error threshold that triggers an errored frame event. • Errored Frame: The number of detected error frames over the specific detection interval. • Error Running Total: The total number of error frames. • Event Running Total: The total number of errored frame events that have occurred.

oam enable

Syntax

oam enable

undo oam enable

View

Ethernet port view

Default Level

2: System level

Parameters

None

Description

Use the **oam enable** command to enable Ethernet OAM on the Ethernet port.

Use the **undo oam enable** command to disable Ethernet OAM on the Ethernet port.

By default, Ethernet OAM is disabled on all Ethernet ports.

Examples

Enable OAM on port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam enable
```

oam errored-frame period

Syntax

oam errored-frame period *period-value*

undo oam errored-frame period

View

System view

Default Level

2: System level

Parameters

period-value: Errored frame detection interval, ranging from 1 to 60 (in seconds).

Description

Use the **oam errored-frame period** command to set the errored frame detection interval.

Use the **undo oam errored-frame period** command to restore the default.

By default, the errored frame detection interval is one second.

Related commands: **oam errored-frame threshold**, **display oam link-event**, **display oam configuration**.

Examples

Set the errored frame detection interval to 10 seconds.

```
<Sysname> system-view
[Sysname] oam errored-frame period 10
```

oam errored-frame threshold

Syntax

oam errored-frame threshold *threshold-value*

undo oam errored-frame threshold

View

System view

Default Level

2: System level

Parameters

threshold-value: Errored frame event triggering threshold, ranging from 0 to 4294967295.

Description

Use the **oam errored-frame threshold** command to set the errored frame event triggering threshold.

Use the **undo oam errored-frame threshold** command to restore the default.

By default, the errored frame event triggering threshold is 1.

Related commands: **oam errored-frame period**, **display oam link-event**, **display oam configuration**.

Examples

Set the errored frame event triggering threshold to 100.

```
<Sysname> system-view
[Sysname] oam errored-frame threshold 100
```

oam errored-frame-period period

Syntax

oam errored-frame-period period *period-value*

undo oam errored-frame-period period

View

System view

Default Level

2: System level

Parameters

period-value: Errored frame period detection interval, ranging from 100 to 60000 (in milliseconds).

Description

Use the **oam errored-frame-period period** command to set the errored frame period detection interval.

Use the **undo oam errored-frame-period period** command to restore the default.

By default, the errored frame period detection interval is 1000 milliseconds.

As for errored frame period event detection, the system first uses the following expression to convert the errored frame period detection interval to the maximum number of 64-byte frames that can be transmitted through an Ethernet port in the period:

bandwidth * period / (64 * 8 * 1000),

where **bandwidth** is the port bandwidth (in bps) and “period” is the configured period (in milliseconds).

Related commands: **oam errored-frame-period threshold**, **display oam link-event**, **display oam configuration**.

Examples

Set the errored frame period detection interval to 10 seconds, that is, 10000 milliseconds.

```
<Sysname> system-view
[Sysname] oam errored-frame-period period 10000
```

oam errored-frame-period threshold

Syntax

oam errored-frame-period threshold *threshold-value*

undo oam errored-frame-period threshold

View

System view

Default Level

2: System level

Parameters

threshold-value: Errored frame period event triggering threshold, ranging from 0 to 4294967295.

Description

Use the **oam errored-frame-period threshold** command to set the errored frame period event triggering threshold.

Use the **undo oam errored-frame-period threshold** command to restore the default.

By default, the errored frame period event triggering threshold is 1.

Related commands: **oam errored-frame-period period**, **display oam link-event**, **display oam configuration**.

Examples

Set the errored frame period event triggering threshold to 100.

```
<Sysname> system-view
[Sysname] oam errored-frame-period threshold 100
```

oam errored-frame-seconds period

Syntax

oam errored-frame-seconds period *period-value*

undo oam errored-frame-seconds period

View

System view

Default Level

2: System level

Parameters

period-value: Errored frame seconds detection interval, ranging from 10 to 900 (in seconds).

Description

Use the **oam errored-frame-seconds period** command to set the errored frame seconds detection interval.

Use the **undo oam errored-frame-seconds period** command to restore the default.

By default, the errored frame seconds detection interval is 60 seconds.

Related commands: **oam errored-frame-seconds threshold**, **display oam link-event**, **display oam configuration**.

Examples

Set the errored frame seconds detection interval to 100 seconds.

```
<Sysname> system-view
[Sysname] oam errored-frame-seconds period 100
```

oam errored-frame-seconds threshold

Syntax

oam errored-frame-seconds threshold *threshold-value*

undo oam errored-frame-seconds threshold

View

System view

Default Level

2: System level

Parameters

threshold-value: Errored frame seconds event triggering threshold, ranging from 0 to 900.

Description

Use the **oam errored-frame-seconds threshold** command to set the errored frame seconds event triggering threshold.

Use the **undo oam errored-frame-seconds threshold** command to restore the default.

By default, the errored frame seconds event triggering threshold is 1.

Related commands: **oam errored-frame-seconds period**, **display oam link-event**, **display oam configuration**.

Examples

Set the errored frame seconds event triggering threshold to 100.

```
<Sysname> system-view
[Sysname] oam errored-frame-seconds threshold 100
```

oam errored-symbol period

Syntax

oam errored-symbol period *period-value*

undo oam errored-symbol period

View

System view

Default Level

2: System level

Parameters

period-value: Errored symbol detection interval, ranging from 1 to 60 (in seconds).

Description

Use the **oam errored-symbol period** command to set the errored symbol detection interval.

Use the **undo oam errored-symbol period** command to restore the default.

By default, the errored symbol detection interval is one second.

Related commands: **oam errored-symbol threshold**, **display oam link-event**, **display oam configuration**.

Examples

Set the errored symbol detection interval to 10 seconds.

```
<Sysname> system-view
[Sysname] oam errored-symbol period 10
```

oam errored-symbol threshold

Syntax

oam errored-symbol threshold *threshold-value*

undo oam errored-symbol threshold

View

System view

Default Level

2: System level

Parameters

threshold-value: Errored symbol event triggering threshold, ranging from 0 to 4,294,967,295.

Description

Use the **oam errored-symbol threshold** command to set the errored symbol event triggering threshold.

Use the **undo oam errored-symbol threshold** command to restore the default.

By default, the errored symbol event triggering threshold is 1.

Related commands: **oam errored-symbol period**, **display oam link-event**, **display oam configuration**.

Examples

Set the errored symbol event triggering threshold to 100.

```
<Sysname> system-view
[Sysname] oam errored-symbol threshold 100
```

oam loopback

Syntax

oam loopback

undo oam loopback

View

Ethernet port view

Default Level

2: System level

Parameters

None

Description

Use the **oam loopback** command to enable Ethernet OAM loopback testing on an Ethernet port.

Use the **undo loopback** command to disable Ethernet OAM remote loopback.

By default, Ethernet OAM loopback testing is disabled.

Ethernet OAM remote loopback is available only after the Ethernet OAM connection is established and can be performed only by the Ethernet OAM entities operating in active Ethernet OAM mode.

Related commands: **oam enable**, **oam mode**.

Examples

Configure the active Ethernet OAM mode, enable Ethernet OAM, and enable Ethernet OAM remote loopback on GigabitEthernet1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] oam mode active
[Sysname-GigabitEthernet1/0/1] oam enable
[Sysname-GigabitEthernet1/0/1] oam loopback
```

oam mode

Syntax

oam mode { **active** | **passive** }

View

Ethernet port view

Default Level

2: System level

Parameters

active: Specifies the active Ethernet OAM mode.

passive: Specifies the passive Ethernet OAM mode.

Description

Use the **oam mode** command to set the Ethernet OAM operating mode for an Ethernet port.

By default, an Ethernet OAM-enabled Ethernet port operates in the active Ethernet OAM mode.

Note that, to change the Ethernet OAM operating mode of an Ethernet OAM-enabled Ethernet port, you need to disable Ethernet OAM on the port first..

Related commands: **oam enable**.

Examples

Disable Ethernet OAM on Gigabitethernet 1/0/1, and then configure Gigabitethernet 1/0/1 to operate in passive Ethernet OAM mode.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo oam enable
[Sysname-GigabitEthernet1/0/1] oam mode active
```

reset oam

Syntax

reset oam [**interface** *interface-type interface-number*]

View

User view

Default Level

2: System level

Parameters

interface *interface-type interface-number*: Specify a port by its type and number.

Description

Use the **reset oam** command to clear the statistics on Ethernet OAM packets and Ethernet OAM link error events of an Ethernet port.

If you do not specify the **interface** keyword, this command clears the statistics on Ethernet OAM packets and Ethernet OAM link error events of all the ports.

Related commands: **display oam**, **display oam link-event**.

Examples

Clear the statistics on Ethernet OAM packets and Ethernet OAM link error events of all the ports.

```
<Sysname> reset oam
```

6 Connectivity Fault Detection Configuration Commands

Connectivity Fault Detection Configuration Commands

cfd cc enable

Syntax

cfd cc service-instance *instance-id* **mep** *mep-id* **enable**

undo cfd cc service-instance *instance-id* **mep** *mep-id* **enable**

View

Ethernet port view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

mep *mep-id*: Specifies the ID of an MEP, ranging from 1 to 8191.

Description

Use the **cfd cc enable** command to enable CCM sending on a specified MEP.

Use the **undo cfd cc enable** command to cancel the configuration.

By default, the CCM sending function is disabled.

Related commands: **cfd cc interval**.

Examples

On port GigabitEthernet 1/0/1, Enable CCM sending on service point 3.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cfd cc service-instance 5 mep 3 enable
```

cfd cc interval

Syntax

cfd cc interval *interval-field-value* **service-instance** *instance-id*

undo cfd cc interval service-instance *instance-id*

View

System view

Default level

2: System level

Parameters

interval-field-value: Value of the interval field in CCM messages, ranging from 4 to 7.

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

Description

Use the **cfd cc interval** command to set the value of the interval field in the CCM messages.

Use the **undo cfd cc interval** command to restore the value to the default value.

By default, the value of this field is 4 for all CCMs sent.

The relationship between the interval field value in the CCM messages, the time interval to send CCM messages and the timeout time of the remote MEP is illustrated in Table 6-1.

Table 6-1 Relationship of interval field value, time interval for sending CCMs and timeout time of remote MEP

Interval field value	Time interval for CCM	Timeout time of remote MEP
4	1 second	3.5 seconds
5	10 second	35 seconds
6	60 seconds	210 seconds
7	600 seconds	2100 seconds

Related commands: **cfd cc enable**.

Examples

Set the value of the interval field in CCMs to 7.

```
<Sysname> system-view
[Sysname] cfd cc interval 7 service-instance 2
```

cfd enable

Syntax

cfd enable

undo cfd enable

View

System view

Default level

2: System level

Parameters

None

Description

Use the **cfd enable** command to enable CFD.

Use the **undo cfd enable** command to disable CFD.

By default, CFD is disabled.

Examples

Enable CFD.

```
<Sysname> system-view
[Sysname] cfd enable
Note: CFD has been enabled.
```

cfd linktrace

Syntax

cfd linktrace service-instance *instance-id* **mep** *mep-id* { **target-mep** *target-mep-id* | **target-mac** *mac-address* } [**ttl** *ttl-value*] [**hw-only**]

View

System view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

mep *mep-id*: Specifies the ID of the MEP that sends LTMs, ranging from 1 to 8191.

target-map *target-mep-id*: Specifies the ID of the MEP that receives LTM, ranging from 1 to 8191.

target-mac *mac-address*: Specifies the destination MAC address, in the format of H-H-H.

ttl *ttl-value*: Specifies the time to live value, ranging from 1 to 255 and defaulting to 64.

hw-only: Indicates the hw-only position of the LTMs sent. When this keyword is present and the MIP that receives LTMs cannot find the destination MAC address in its forwarding table, the MIP will not forward these broadcast messages. Otherwise, the LTMs will be forwarded.

Description

Use the **cfd linktrace** command to find the path between the specified MEP and the destination MEP, which is achieved through the transmission of LTMs between the two and detection of the responding LTRs.

Related commands: **cfd linktrace auto-detection**.

Examples

Send LTM messages.

```
<Sysname> system-view
```

```
[Sysname] cfd linktrace service-instance 1 mep 1101 target-mep 2001
Linktrace to MEP 2001 with the sequence number 1101-43361 :
MAC Address             TTL     Forwarded       Relay Action
0010-FC00-6512          63      No              None
```

Table 6-2 cfd linktrace command output description

Field	Description
Linktrace to MEP *mep-id* with the sequence number *sequence-number*	Linktrace to MEP *mep-id* with the sequence number *sequence-number*
MAC Address	Source MAC address in the LTR messages
TTL	Hop count when the LTM passes the device
Forwarded	• Yes means that the current device forwards LTMs. • No means that the current device does not forward LTMs.
Relay Action	Indicates whether the forwarding device found the destination MAC address in its MAC address table. • Found: Indicates that the forwarding device found the destination MAC address in its MAC address table. • Unknown: Indicates that the forwarding device failed to find the destination MAC address in its MAC address table. • None: Indicates that it is a MEP that responded to the LTM message. A MEP does not need to find the destination MAC address.

cfd linktrace auto-detection

Syntax

cfd linktrace auto-detection [**size** *size-value*]

undo cfd linktrace auto-detection

View

System view

Default level

2: System level

Parameters

size *size-value*: Specifies the size of the buffer used to store the auto-detection result, ranging from 1 to 100 (in terms of sending times).

This value defaults to 5, which means the buffer stores the results of the recent five auto-detections.

Description

Use the **cfd linktrace auto-detection** command to enable the auto sending of linktrace messages.

Use the **undo cfd linktrace auto-detection** command to disable this function.

By default, this function is disabled.

Note that:

- After LT messages automatic sending is enabled, if a MEP fails to receive the CCMs from the remote MEP, the link between the two is regarded as faulty and LTMs will be sent out. (The destination of the LTMs is the remote MEP, and the maximum value of TTL is 255.) Based on the LTRs that echo back, the fault source can be located.
- Once you disable LT messages automatic sending, the content stored in the buffer will be removed.

Related commands: **cfd linktrace**.

Examples

Enable automatic LT messages sending.

```
<Sysname> system-view
[Sysname] cfd linktrace auto-detection size 100
```

cfd loopback

Syntax

cfd loopback service-instance *instance-id* **mep** *mep-id* { **target-mep** *target-mep-id* | **target-mac** *mac-address* } [**number** *number*]

View

System view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

mep *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

target-mep *target-mep-id*: Specifies the ID of the destination MEP for LBM packets, ranging from 1 to 8191.

target-mac *mac-address*: Specifies the destination MAC address, in the format of H-H-H.

number *number*: Specifies the number of the LBMs packets sent, ranging from 1 to 10 and defaulting to 5.

Description

Use the **cfd loopback** command to enable LB function so that LBMs can be sent from the specified MEP to other MEPs in the same service instance, and LBR messages can be received.

By default, LB is not enabled.

Examples

Enable LB to check link state.

```
<Sysname> system-view
[Sysname] cfd loopback service-instance 1 mep 1101 target-mep 2001
Loopback to 0010-FC00-6512 with the sequence number start from 1101-43404:
```

```
Reply from 0010-FC00-6512: sequence number=1101-43404
Reply from 0010-FC00-6512: sequence number=1101-43405
Reply from 0010-FC00-6512: sequence number=1101-43406
Reply from 0010-FC00-6512: sequence number=1101-43407
Reply from 0010-FC00-6512: sequence number=1101-43408
Send:5       Received:5       Lost:0
```

Table 6-3 cfd loopback command output description

Field	Description
Loopback to *mac-address* with the sequence number start from *sequence-number*	Sends LBMs to *mac-address* with the sequence number starting with *sequence-number*
Reply from *mac-address*	Reply from *mac-address*
sequence number	Sequence number in the LBR messages
Send	Number of LBMs sent
Received	Number of LBR messages received
Lost	Number of lost LBMs

cfd ma

Syntax

cfd ma *ma-name* **md** *md-name* **vlan** *vlan-id*

undo cfd ma *ma-name* **md** *md-name*

View

System view

Default level

2: System level

Parameters

ma-name: Name of the MA, a string of 1 to 48 characters, composed of letters, numbers or underlines, but cannot start with an underline character.

md *md-name*: Specifies the name of an MD, a string of 1 to 48 characters, composed of letters, numbers or underlines, but cannot start with an underline character.

vlan *vlan-id*: Specifies the ID of the VLAN where MA is in service, ranging from 1 to 4094.

Description

Use the **cfd ma** command to create MA(s) in an MD.

Use the **undo cfd ma** command to delete specified MA in an MD.

By default, no MA is created.

Note that:

- Before creating an MA, you must create an MD first.
- When deleting an MA, you will also delete the configurations related to that MA.

Related commands: **cfd md**.

Examples

Create an MA named **test_ma** in an MD named **test_md**, and configure the MD to serve VLAN 100.

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
[Sysname] cfd ma test_ma md test_md vlan 100
```

cfd md

Syntax

cfd md *md-name* **level** *level-value*

undo cfd md *md-name*

View

System view

Default level

2: System level

Parameters

md *md-name*: Name of an MD, a string of 1 to 48 characters, composed of letters, numbers or underlines, but cannot start with an underline character.

level *level-value*: Specifies an MD level, ranging from 0 to 7.

Description

Use the **cfd md** command to create an MD.

Use the **undo cfd md** command to delete an MD.

By default, no MD is created.

Note that:

- You can create only one MD with a specific level. MD cannot be created if you enter an invalid MD name or an existing MD name.
- When deleting an MD, you will also delete the configurations related to that MD.

Examples

Create an MD named **test_md**, with its level being 3.

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
```

cfd mep

Syntax

cfd mep *mep-id* **service-instance** *instance-id* { **inbound | outbound** }

undo cfd mep *mep-id* **service-instance** *instance-id*

View

Ethernet port view

Default level

2: System level

Parameters

mep *mep-id*: ID of MEP, ranging from 1 to 8191.

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

inbound: Creates an inward-facing MEP.

outbound: Creates an outward-facing MEP.

Description

Use the **cfd mep** command to create a MEP on a port.

Use the **undo cfd mep** command to delete the specified MEP.

By default, no MEP is configured on a device port.

In creating a MEP, the service instance you specified defines the MD and MA that the MEP belongs to.

Examples

Create inward-facing MEP 3 in service instance 5.

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
[Sysname] cfd ma test_ma md test_md vlan 100
[Sysname] cfd service-instance 5 md test_md ma test_ma
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cfd mep 3 service-instance 5 inbound
```

cfd mep enable

Syntax

cfd mep service-instance *instance-id* **mep** *mep-id* **enable**

undo cfd mep service-instance *instance-id* **mep** *mep-id* **enable**

View

Ethernet port view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

mep *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

Description

Use the **cfd mep enable** command to enable the MEP configured on a port.

Use the **undo cfd mep enable** command to disable the MEP.

By default, MEP is disabled on a port and cannot respond to LTM and LBM messages unless you enable it.

Related commands: **cfd mep**.

Examples

Enable MEP 3 in service instance 5.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cfd mep service-instance 5 mep 3 enable
```

cfd mip-rule

Syntax

cfd mip-rule { **explicit** | **default** } **service-instance** *instance-id*

undo cfd mip-rule service-instance *instance-id*

View

System view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

explicit: This rule means that if the lower level MA is not configured with MIPs, whether the current MA will create MIPs depends on whether the lower level MA is configured with MEPs.

default: This rule means that if the lower level MA is not configured with MIPs, the current MA will create MIPs.

Description

Use the **cfd mip-rule** command to configure the rule for generating MIPs.

Use the **undo cfd mip-rule** command to delete the rule for generating MIPs.

By default, no rules for generating MIPs are configured, nor are the MIPs themselves.

MIPs are generated on each port automatically according to the rules configured. If a port has no MIP, the system will check the MAs in each MD (from low to high level), and follow the rules in Table 6-4 to create or not create MIPs (within a single VLAN):

Table 6-4 Rules for generating MIPs

MIP exists on low level MA	The cfd mip-rule command is configured as	MEP exists on low level MA	Create MIP or not
Yes	—	—	No
No	**Explicit**	No	No
		Yes	Yes
	Default	—	Yes

Each of the following actions or cases can cause MIPs to be created or deleted after you have configured this command:

- Enabling CFD (use the **cfd enable** command)
- Creating or deleting the MEPs on a port
- Changes occur to the VLAN attribute of a port
- The rule specified in the **cfd mip-rule** command changes

Examples

Configure the rules for generating MIPs.

```
<Sysname> system-view
[Sysname] cfd mip-rule default service-instance 5
```

cfd remote-mep

Syntax

cfd remote-mep *remote-mep-id* **service-instance** *instance-id* **mep** *mep-id*

undo cfd remote-mep *remote-mep-id* **service-instance** *instance-id* **mep** *mep-id*

View

Ethernet port view

Default level

2: System level

Parameters

remote-mep-id: ID of the remote MEP, ranging from 1 to 8191.

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

mep *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

Description

Use the **cfd remote-mep** command to configure the remote MEP for the specified local MEP (the two must be in the same service instance) on the local port. After this, the local MEP can receive CCMs from the remote MEP.

Use the **undo cfd remote-mep** command to delete the remote MEP configured on the local port.

Note that the remote MEP ID and local MEP ID cannot be the same.

Examples

Configure a remote MEP.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] cfd remote-mep 9 service-instance 5 mep 3
```

cfd service-instance

Syntax

cfd service-instance *instance-id* **md** *md-name* **ma** *ma-name*

undo cfd service-instance *instance-id*

View

System view

Default level

2: System level

Parameters

service-instance *instance-id*: Service instance ID, ranging from 1 to 32767.

md *md-name*: Specifies the name of an MD, a string of 1 to 48 characters, composed of letters, numbers or underlines, but cannot start with an underline character.

ma *ma-name*: Specifies the name of an MA, a string of 1 to 48 characters, composed of letters, numbers or underlines, but cannot start with an underline character.

Description

Use the **cfd service-instance** command to create a service instance.

Use the **undo cfd service-instance** command to delete a service instance.

By default, no service instance is created.

Note that:

- You must create MD and MA prior to creating service instance.
- The service instance ID uniquely identifies an MA in an MD.
- When deleting a service instance, you are deleting the configurations related to that service instance as well.
- Deleting a service instance simply breaks up the connection between the service instance and the corresponding MA, the MA itself is not deleted.

Related commands: **cfd md**, **cfd ma**.

Examples

Create service instance 5, an MD named **test_md**, and an MA named **test_ma**.

```
<Sysname> system-view
[Sysname] cfd md test_md level 3
[Sysname] cfd ma test_ma md test_md vlan 100
[Sysname] cfd service-instance 5 md test_md ma test_ma
```

display cfd linktrace-reply

Syntax

display cfd linktrace-reply [**service-instance** *instance-id* [**mep** *mep-id*]]

View

Any view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

mep *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

Description

Use the **display cfd linktrace-reply** command to display the LTR information received by a MEP.

Note that:

- If this command is used without specifying MEP, the information of LTRs of all MEPs in the current service instance is displayed.
- If this command is used without specifying service instance, the information of LTRs of all MEPs is displayed.

Examples

Display the information of LTR message.

```
<Sysname> display cfd linktrace-reply
Service instance: 1      MEP ID: 1003
MAC Address             TTL    Forwarded       Relay Action
00E0-FC27-6502           63     Yes            Found
00E0-FC00-6510           62     Yes            Found
00E0-FC52-BAA0           61     No             None

Service instance: 2      MEP ID: 1023
MAC Address             TTL    Forwarded       Relay Action
00E0-FC27-6502           63     No             None
```

Table 6-5 display cfd linktrace-reply command output description

Field	Description
Service instance	Service instance to which the MEPs that send LTMs belong
MEP ID	ID of the MEP that sends LTMs
MAC Address	Source MAC address in the LTR message
TTL	Hop count when LTM passes the device
Forwarded	• Yes means that the device has forwarded the LTMs. • No means that the device did not forward the LTMs.

Field	Description
Relay Action	Indicates whether the forwarding device found the destination MAC address in its MAC address table • Found: Indicates that the forwarding device found the destination MAC address in its MAC address table. • Unknown: Indicates that the forwarding device failed to find the destination MAC address in its MAC address table. • None: Indicates that it is a MEP that responded to the LTM message. A MEP does not need to find the destination MAC address.

display cfd linktrace-reply auto-detection

Syntax

display cfd linktrace-reply auto-detection [**size** *size-value*]

View

Any view

Default level

2: System level

Parameters

size *size-value*: Specifies the times of recent auto-detections, ranging from 1 to 100.

Description

Use the **display cfd linktrace-reply auto-detection** command to display the content of the LTR messages received as responses to the automatically sent LTMs.

Note that:

- These LTR messages are stored in the buffer after you executed the **cfd linktrace auto-detection** command.
- With the **size** keyword not specified, this command displays the information of all LTRs stored in the buffer.

Related commands: **cfd linktrace auto-detection.**

Examples

Display the content of the LTRs received as responses to the LTMs sent.

```
<Sysname> display cfd linktrace-reply auto-detection
Service instance: 1      MEP ID: 1003    Time: 2006/05/22 10:43:57
Target MEP ID: 2005      TTL: 64
MAC Address             TTL     Forwarded        Relay Action
00E0-FC27-6502           63      Yes             Found
00E0-FC00-6510           62      Yes             Found
00E0-FC52-BAA0           61      No              None

Service instance: 2      MEP ID: 1023    Time: 2006/05/22 10:44:06
Target MEP ID: 2025      TTL: 64
```

```
MAC Address             TTL       Forwarded       Relay Action
00E0-FC27-6502          63        No              None
```

Table 6-6 display cfd linktrace-reply auto-detection command output description

Field	Description
Service instance	Service instance to which the MEPs that sent LTM messages belong
MEP ID	ID of the MEP that sends LTMs
Time	Time of the LTMs automatically sent
Target MEP ID	ID of the target MEP
TTL	Initial hop count of the automatically sent LTMs
MAC Address	Source MAC address in the LTR messages
TTL	Hop count when LTM passes the device
Forwarded	• Yes means that the device has forwarded the LTMs. • No means that the device did not forward the LTMs.
Relay Action	Indicates whether the forwarding device found the destination MAC address in its MAC address table. • Found: Indicates that the forwarding device found the destination MAC address in its MAC address table. • Unknown: Indicates that the forwarding device failed to find the destination MAC address in its MAC address table. • None: Indicates that it is a MEP that responded to the LTM message. A MEP does not need to find the destination MAC address.

display cfd ma

Syntax

display cfd ma [[*ma-name*] **md** *md-name*]

View

Any view

Default level

2: System level

Parameters

ma-name: Name of MA, ranging from 1 to 48 characters, composed of letters, numbers or underlines, but cannot start with an underline character.

md *md-name*: Specifies the name of an MD, ranging from 1 to 48 characters, composed of letters, numbers or underlines, but cannot start with an underline character.

Description

Use the **display cfd ma** command to display the configuration of a specified MA.

Note that:

- If MD is not specified, this command will display the MA configurations of all MDs on the device.
- If both MD and MA are specified, this command will display the specified MA configuration.

- If only MD is specified, this command will display the configurations of all MAs in that MD.

Examples

Display the MA configuration information.

```
<Sysname> display cfd ma
3 maintenance domain(s) configured.
Maintenance domain: mdtest_5
1 maintenance association(s) belong(s) to maintenance domain mdtest_5:
Maintenance association: matest_5
Service instance: 5        VLAN: 5        Level: 5

Maintenance domain: mdtest_6
1 maintenance association(s) belong(s) to maintenance domain mdtest_6:
Maintenance association: matest_6
Service instance: 6        VLAN: 6        Level: 6

Maintenance association: matest_16
Service instance: 0        VLAN: 100      Level: 6

Maintenance domain: mdtest_7
1 maintenance association(s) belong(s) to maintenance domain mdtest_7:
Maintenance association: matest_7
Service instance: 7        VLAN: 7        Level: 7
```

Table 6-7 display cfd ma command output description

Field	Description
3 maintenance domain(s) configured.	Number of MDs configured
Maintenance domain	Name of the MD
1 maintenance association(s) belong(s) to maintenance domain mdtest_5	Number of MAs configured in the MD
Maintenance association	Name of the MA
Service instance	Service instance of the MA
VLAN	VLAN to which the service instance belongs
Level	Level of the MD to which the MA belongs

display cfd md

Syntax

display cfd md

View

Any view

Default level

2: System level

Parameters

None

Description

Use the **display cfd md** command to display the MD configuration information.

Examples

Display the MD configuration information.

```
<Sysname> display cfd md
CFD is enabled.
8 maintenance domain(s) configured:
Level: 0    Maintenance domain: mdtest_0
Level: 1    Maintenance domain: mdtest_1
Level: 2    Maintenance domain: mdtest_2
Level: 3    Maintenance domain: mdtest_3
Level: 4    Maintenance domain: mdtest_4
Level: 5    Maintenance domain: mdtest_5
Level: 6    Maintenance domain: mdtest_6
Level: 7    Maintenance domain: mdtest_7
```

Table 6-8 display cfd md command output description

Field	Description
8 maintenance domain(s) configured	Number of MDs configured
Level	Level of MD, each level allows only one MD.
Maintenance domain	Name of MD

display cfd mep

Syntax

display cfd mep *mep-id* **service-instance** *instance-id*

View

Any view

Default level

2: System level

Parameters

mep-id: MEP ID, ranging from 1 to 8191.

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

Description

Use the **display cfd mep** command to display the attribute and operating information of MEP(s).

Examples

Display the attribute and operating information of MEP 50 in service instance 1.

```
<Sysname> display cfd mep 50 service-instance 1
Interface: GigabitEthernet1/0/2
Maintenance domain: mdtest_1
Maintenance association: matest_1
Level: 1       VLAN: 1       Direction: Outbound
Administrative state: Active        CCM send: Enable
FNG state: FNG_DEFECT_REPORTED

CCM:
Current state: CCI_WAITING
Interval: 1s      SendCCM: 12018

Loopback:
NextSeqNumber: 8877
SendLBR: 0        ReceiveInOrderLBR: 0        ReceiveOutOrderLBR: 0

Linktrace:
NextSeqNumber: 8877
SendLTR: 0        ReceiveLTM: 0

No CCM from some remote MEPs is received.

One or more streams of error CCMs is received. The last-received CCM:
Maintenance domain:mdtest1
Maintenance association:matest1
MEP:5     Sequence Number:0x50A
MAC Address: 000F-E25D-F31B
Received Time: 2008/04/26 12:51:31

One or more streams of cross-connect CCMs is received. The last-received CCM:
Maintenance domain:mdtest1
Maintenance association:matest1
MEP:6     Sequence Number:0x63A
MAC Address: 000F-E25D-578C
Received Time: 2008/04/26 12:51:33

Some other MEPs are transmitting the RDI bit.
```

Table 6-9 display cfd mep command output description

Field	Description
Interface	Interface that an MD belongs to

Field	Description
Maintenance domain	MD that a MEP belongs to
Maintenance association	MA that a MEP belongs to
Level	Level of the MD
VLAN	VLAN that the MA belongs to
Direction	Direction of the MEPs
Administrative state	State of MEP, either Active or Inactive
CCM send	Whether the MEP sends CCM
FNG state	State of FNG (Fault Notification Generator), which can be: • FNG_RESET • FNG_DEFECT • FNG_REPORT_DEFECT, • FNG_DEFECT_REPORTED • FNG_DEFECT_CLEARING
CCM	Information related to CCM
Current state	State of CCMs sent, which can be: • CCI_IDLE • CCI_WAITING
Interval	Interval to send CCM
SendCCM	Number of CCMs that have been sent by the MEPs
Loopback	Information related to Loopback
NextSeqNumber	Sequence number of the next LBM to be sent
SendLBR	Number of LBRs that have been sent
ReceiveInOrderLBR	Number of LBR messages received in correct sequence
ReceiveOutOrderLBR	Number of LBR messages received out of order
Linktrace	Information related to linktrace
NextSeqNumber	Sequence number of the next LTM to be sent
SendLTR	Number of LTRs sent
ReceiveLTM	Number of LTMs received
No CCM from some remote MEPs is received.	Failure to receive CCMs from some remote MEPs (This information is displayed only when some CCMs are lost.)
One or more streams of error CCMs is received. The last-received CCM:	Display the content of the last CCM when one or more error CCMs are received. (This information is displayed only when error CCM(s) is/are received.)
Maintenance domain	MD of the last error CCM message
Maintenance association	MA of the last error CCM message
MEP	ID of the MEP that sent the last error CCM message
Sequence Number	Sequence number of the last error CCM
MAC Address	MAC address of the peer that sent the error CCM message
Received Time	Time when the last error CCM is received

Field	Description
One or more streams of cross-connect CCMs is received. The last-received CCM:	Cross-connect CCMs are received, and the content of the last cross-connect CCM is displayed. (This information is displayed only when cross-connect CCM(s) is/are received.)
Some other MEPs are transmitting the RDI bit.	CCMs with RDI bits misplaced are received from other MEPs. (This information is displayed only when this type of CCM(s) is/are received.)

display cfd mp

Syntax

display cfd mp [**interface** *interface-type interface-number*]

View

Any view

Default level

1: Monitor level

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

Description

Use the **display cfd mp** command to display the MP information.

Note that:

- If no port is specified, this command displays the MP information on all ports.
- The information displayed is sorted by port name primarily in the ascending VLAN ID order within the same port, and in the order of outward-facing MEPs (from low to high level), MIPs, and inward-facing MEPs (from high to low level) within the same VLAN.

Examples

Display the MP information on all ports.

```
<Sysname> display cfd mp
Interface GigabitEthernet1/0/1   VLAN 100
MEP ID: 100     Level: 0   Service instance: 100   Direction: Outbound
Maintenance domain: mdtest0
Maintenance association: mainmd0

MEP ID: 105     Level: 5   Service instance: 105   Direction: Outbound
Maintenance domain: mdtest5
Maintenance association: mainmd5

MIP           Level: 6   Service instance: 106
Maintenance domain: mdtest6
Maintenance association: mainmd6
```

```
MEP ID: 104     Level: 4    Service instance: 104    Direction: Inbound
Maintenance domain: mdtest4
Maintenance association: mainmd4

MEP ID: 102     Level: 2    Service instance: 102    Direction: Inbound
Maintenance domain: mdtest2
Maintenance association: mainmd2

Interface GigabitEthernet1/0/4   VLAN 1
MEP ID: 9       Level: 6    Service instance: 6     Direction: Outbound
Maintenance domain: mdtest6
Maintenance association: matest6
```

Table 6-10 display cfd mp command output description

Field	Description
Interface GigabitEthernet1/0/1 VLAN 100	MP configuration of the specified VLAN on the specified port
MEP ID	ID of the MEP
MIP	A MIP in the MP
Level	MD level that an MP belongs to
Service instance	Service instance to which the MP belongs
Direction	Direction of the MP
Maintenance domain	MD to which an MP belongs
Maintenance association	MA to which an MP belongs

display cfd remote-mep

Syntax

display cfd remote-mep service-instance *instance-id* **mep** *mep-id*

View

Any view

Default level

2: System level

Parameters

service-instance *instance-id*: Specifies the service instance ID, ranging from 1 to 32767.

mep *mep-id*: Specifies the ID of a MEP, ranging from 1 to 8191.

Description

Use the **display cfd remote-mep** command to display the information of the remote MEP.

Examples

Display the information of remote MEP 10 in service instance 4.

```
<Sysname> display cfd remote-mep service-instance 4 mep 10
MEP ID   MAC Address     State       Time               MAC Status
20       00E0-FC00-6565  OK          2006/03/06 02:36:38   UP
30       00E0-FC27-6502  OK          2006/03/06 02:36:38   DOWN
40       00E0-FC00-6510  FAILED      2006/03/06 02:36:39   DOWN
50       00E0-FC52-BAA0  OK          2006/03/06 02:36:44   DOWN
60       0010-FC00-6502  OK          2006/03/06 02:36:42   DOWN
```

Table 6-11 display cfd remote-mep command output description

Field	Description
MEP ID	ID of the remote MED
MAC Address	MAC address of the remote MEP device
State	Running state of MEP, either OK or FAILED
Time	Recent time of the remote MEP when it is FAILED or OK.
MAC Status	State of the port indicated by the last CCM received from the remote MEP, either UP or DOWN

display cfd service-instance

Syntax

display cfd service-instance [*instance-id*]

View

Any view

Default level

2: System level

Parameters

instance-id: Service instance, ranging from 1 to 32767.

Description

Use the **display cfd service-instance** command to display the configuration information of service instance.

Without specifying the service instance ID, the command will display the configuration information of all service instances. With service instance ID specified, this command will display the configuration information of the specified service instance.

Examples

Display the service instance configuration information.

```
<Sysname> display cfd service-instance
2 service instance(s) configured:
```

```
Service instance 5:
Maintenance domain: mdtest_5
Maintenance association: matest_5
Level: 5       VLAN: 5       MIP rule: None        CCM interval: 1s

Service instance 6:
Maintenance domain: mdtest_6
Maintenance association: matest_6
Level: 6       VLAN: 6       MIP rule: None        CCM interval: 1s

<Sysname> display cfd service-instance 7
Service instance 7:
Maintenance domain: mdtest_7
Maintenance association: matest_7
Level: 7       VLAN: 7       MIP rule: None        CCM interval: 1s
MEP ID: 731    Interface: GigabitEthernet1/0/1            Direction: Inbound
```

Table 6-12 display cfd service-instance command output description

Field	Description
2 service instance(s) are configured.	Number of service instance configured.
Service instance 5	Service instance ID
Maintenance domain	MD of the service instance
Maintenance association:	MA of the service instances
Level	MD level
VLAN	VLAN that the MA belongs to
MIP rule	MIP generation rules configured on service instance
CCM interval	Interval to send CCMs
MEP ID	ID of MEPs configured on the service instance
Interface	Interface of the MEP configured on the service instance
Direction	Direction of the MEPs configured on the service instance

display cfd status

Syntax

display cfd status

View

Any view

Default level

2: System level

Parameters

None

Description

Use the **display cfd status** command to display the status of CFD (enabled or disabled).

Examples

Display the status of CFD.

```
<Sysname> display cfd status
CFD is enabled.
```

7 Track Configuration Commands

Track Configuration Commands

display track

Syntax

display track { *track-entry-number* | **all** }

View

Any view

Default Level

1: Monitor level

Parameters

track-entry-number: Displays information about the specified Track object, in the range 1 to 1024.

all: Displays information about all the Track objects.

Description

Use the **display track** command to display Track object information.

Examples

Display information about all the Track objects.

```
<Sysname> display track all
Track ID: 1
  Status: Positive
  Reference Object:
    NQA Entry: admin test
    Reaction: 10
```

Table 7-1 display track command output description

Field	Description
Track ID	ID of a Track object
Status	Status of a Track object: • Positive: The Track object is normal. • Invalid: The Track object is invalid. • Negative: The Track object is abnormal.
Reference Object	The objects referenced by the Track object

Field	Description
NQA Entry	The NQA test group referenced by the Track object
Reaction	The Reaction entry referenced by the Track object

track nqa

Syntax

track *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-num*

undo track *track-entry-number*

View

System view

Default Level

2: System level

Parameters

track-entry-number: Track object ID, in the range 1 to 1024.

entry *admin-name operation-tag*: Specifies the NQA test group to be associated with the Track object. *admin-name* is the name of the administrator creating the NQA operation, a string of 1 to 32 characters, case-insensitive. *operation-tag* is the NQA operation tag, a string of 1 to 32 characters, case-insensitive.

reaction *item-num*: Specifies the Reaction entry to be associated with the Track object. *item-num* is the Reaction entry ID, in the range 1 to 10.

Description

Use the **track** command to create the Track object to be associated with the specified Reaction entry of the NQA test group.

Use the **undo track** command to remove the created Track object.

By default, no Track object is created.

Note that after a Track object is created, you cannot modify it using the **track** command.

Related commands: **nqa**, and **reaction** in *NQA Commands* in the *System Volume*.

Examples

Create Track object 1 to associate it with Reaction entry 3 of the NQA test group (admin-test).

```
<Sysname> system-view
[Sysname] track 1 nqa entry admin test reaction 3
```

Table of Contents

1 Commands for Logging into an Ethernet Switch

Commands for Logging into an Ethernet Switch

activation-key

Syntax

activation-key *character*

undo activation-key

View

AUX interface view

Default Level

3: Manage level

Parameters

character: Shortcut key for starting terminal sessions, a character or its ASCII decimal equivalent in the range 0 to 127; or a string of 1 to 3 characters.

Description

Use the **activation-key** command to define a shortcut key for starting a terminal session.

Use the **undo activation-key** command to restore the default shortcut key.

You can use a single character (or its corresponding ASCII code value in the range 0 to 127) or a string of 1 to 3 characters to define a shortcut key. In the latter case, the system takes only the first character to define the shortcut key. For example, if you input an ASCII code value 97, the system will set the shortcut key to <a>; if you input the string **b@c**, the system will set the shortcut key to <b>.

You may use the **display current-configuration** command to verify the shortcut key you have defined.

By default, pressing **Enter** key will start a terminal session.

Examples

Set the shortcut key for starting terminal sessions to <s>.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] activation-key s
```

To verify the configuration, do the following:

Exit the terminal session on the aux port, and enter <s> at the prompt of “Please press ENTER”. You will see the terminal session being started.

```
[Sysname-ui-aux0] return
```

```
<Sysname> quit
******************************************************************************
* Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved. *
* This software is protected by copyright law and international treaties.    *
* Without the prior written permission of 3Com Corporation and its licensors,*
* any reproduction republication, redistribution, decompiling, reverse       *
* engineering is strictly prohibited. Any unauthorized use of this software  *
* or any portion of it may result in severe civil and criminal penalties, and*
* will be prosecuted to the maximum extent possible under the applicable law.*
******************************************************************************
User interface aux0 is available.


Please press ENTER.

<Sysname>
%Apr 28 04:33:11:611 2005 Sysname SHELL/5/LOGIN: Console login from aux0
```

authentication-mode

Syntax

authentication-mode { **none** | **password** | **scheme** }

View

User interface view

Default Level

3: Manage level

Parameters

none: Does not authenticate users.

password: Authenticates users using the local password.

scheme: Authenticates users locally or remotely using usernames and passwords.

Description

Use the **authentication-mode** command to specify the authentication mode.

- If you specify the **password** keyword to authenticate users using the local password, remember to set the local password using the **set authentication password** { **cipher** | **simple** } *password* command.
- If you specify the **scheme** keyword to authenticate users locally or remotely using usernames and passwords, the actual authentication mode depends on other related configuration. Refer to the AAA-RADIUS-HWTACACS module of this manual for more.

After you specify to perform local password authentication, when a user logs in through the Console port, a user can log into the switch even if the password is not configured on the switch. But for a VTY user interface, a password is needed for a user to log into the switch through it under the same condition.

By default, users logging in through the Console port are not authenticated.

Caution

For VTY user interface, if you want to set the login authentication mode to **none** or **password**, you must first verify that the SSH protocol is not supported by the user interface. Otherwise, your configuration will fail. Refer to protocol inbound.

Examples

Configure to authenticate users using the local password.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] authentication-mode password
```

auto-execute command

Syntax

auto-execute command *text*

undo auto-execute command

View

User interface view

Default Level

3: Manage level

Parameters

text: Command to be executed automatically.

Description

Use the **auto-execute command** command to set the command that is executed automatically after a user logs in.

Use the **undo auto-execute command** command to disable the specified command from being automatically executed.

Use these two commands in the VTY user interface only.

Normally, the **telnet** command is specified to be executed automatically to enable the user to Telnet to a specific network device automatically.

By default, no command is automatically executed.

Caution

- The **auto-execute command** command may cause you unable to perform common configuration in the user interface, so use it with caution.
- Before executing the **auto-execute command** command and save your configuration, make sure you can log into the switch in other modes and cancel the configuration.

Examples

Configure the **telnet** 10.110.100.1 command to be executed automatically after users log into VTY 0.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] auto-execute command telnet 10.110.100.1
% This action will lead to configuration failure through ui-vty0. Are you sure?[Y/N]y
```

After the above configuration, when a user logs onto the device through VTY 0, the device automatically executes the configured command and logs off the current user.

command accounting

Syntax

command accounting

undo command accounting

View

User interface view

Default Level

3: Manage level

Parameters

None

Description

Use the **command accounting** command to enable command accounting.

Use the **undo command accounting** command to restore the default.

By default, command accounting is disabled, that is, the accounting server does not record the commands that the users executed.

If command accounting is enabled, every executed command will be recorded on the HWTACACS server.

If both command accounting and command authorization are enabled, only the authorized and executed commands will be recorded on the HWTACACS server.

Examples

Enable command accounting for VTY 0. Then the HWTACACS server records the commands executed by the users logging in from VTY 0.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] command accounting
```

command authorization

Syntax

command authorization

undo command authorization

View

User interface view

Default Level

3: Manage level

Parameters

None

Description

Use the **command authorization** command to enable command authorization.

Use the **undo command authorization** command to restore the default.

By default, command authorization is disabled, that is, logged-in users can execute commands without authorization.

With command authorization enabled, users logging in from the current user interface can perform commands authorized by the server.

Examples

Enable command accounting for VTY 0. Then users logging in through VTY 0 can perform the commands authorized by the HWTACACS server only.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] command authorization
```

databits

Syntax

databits { **5** | **6** | **7** | **8** }

undo databits

View

AUX interface view

Default Level

2: System level

Parameters

5: Five data bits.

6: Six data bits.

7: Seven data bits.

8: Eight data bits.

Description

Use the **databits** command to set the databits for the user interface.

Use the **undo databits** command to revert to the default data bits.

The default data bits is 8.

Note

3COM switch 4210G only support data bits 7 and 8. To establish the connection again, you need to modify the configuration of the termination emulation utility running on your PC accordingly.

Examples

Set the data bits to 7.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] databits 7
```

display telnet client configuration

Syntax

display telnet client configuration

View

Any view

Default Level

1: Monitor level

Parameter

None

Description

Use the **display telnet client configuration** command to display the source IP address or source interface configured for the current device.

Example

Display the source IP address or source interface configured for the current device.

```
<Sysname> display telnet client configuration
 The source IP address is 1.1.1.1.
```

display user-interface

Syntax

display user-interface [*type number* | *number*] [**summary**]

View

Any view

Default Level

1: Monitor level

Parameters

type: User interface type.

number: Absolute or relative index of the user interface. This argument can be an absolute user interface index (if you do not provide the *type* argument) or a relative user interface index (if you provide the *type* argument).

summary: Displays the summary information about a user interface.

Description

Use the **display user-interface** command to view information about the specified or all user interfaces.

When the **summary** keyword is absent, the command will display the type of the user interface, the absolute or relative number, the speed, the user privilege level, the authentication mode and the physical location.

When the **summary** keyword is present, the command will display all the number and type of user interfaces under use and without use.

Examples

Display the information about user interface 0.

```
<Sysname> display user-interface 0
  Idx  Type     Tx/Rx     Modem Privi Auth  Int
F 0    AUX 0    19200       -     3     N     -

  +    : Current user-interface is active.
  F    : Current user-interface is active and work in async mode.
  Idx  : Absolute index of user-interface.
  Type : Type and relative index of user-interface.
```

```
Privi: The privilege of user-interface.
Auth : The authentication mode of user-interface.
Int  : The physical location of UIs.
A    : Authenticate use AAA.
L    : Authentication use local database.
N    : Current UI need not authentication.
P    : Authenticate use current UI's password.
```

Table 1-1 Descriptions on the fields of the **display user-interface** command

Filed	Description
+	The information displayed is about the current user interface.
F	The information displayed is about the current user interface. And the current user interface operates in asynchronous mode.
Idx	The absolute index of the user interface
Type	User interface type and the relative index
Tx/Rx	Transmission speed of the user interface
Modem	Indicates whether or not a modem is used.
Privi	The available command level
Auth	The authentication mode
Int	The physical position of the user interface

display users

Syntax

display users [**all**]

View

Any view

Default Level

1: Monitor level

Parameters

all: Displays the information about all user interfaces.

Description

Use the **display users** command to display the information about user interfaces. If you do not specify the **all** keyword, only the information about the current user interface is displayed.

Examples

Display the information about the current user interface.

```
<Sysname> display users
The user application information of the user interface(s):
  Idx   UI     Delay   Type Userlevel
```

```
  1   VTY 0   00:11:45  TEL  3
  2   VTY 1   00:16:35  TEL  3
  3   VTY 2   00:16:54  TEL  3
+ 4   VTY 3   00:00:00  TEL  3

Following are more details.
VTY 0   :
       Location: 192.168.0.123
VTY 1   :
       Location: 192.168.0.43
VTY 2   :
       Location: 192.168.0.2
VTY 3   :
       User name: user
       Location: 192.168.0.33
 +    : Current operation user.
 F    : Current operation user work in async mode.
```

Table 1-2 Descriptions on the fields of the **display users** command

Field	Description
+	The information displayed is about the current user interface.
F	The information is about the current user interface, and the current user interface operates in asynchronous mode.
UI	The numbers in the left sub-column are the absolute user interface indexes, and those in the right sub-column are the relative user interface indexes.
Delay	The period in seconds the user interface idles for.
Type	User type
Userlevel	The level of the commands available to the users logging into the user interface
Location	The IP address form which the user logs in.
User name	The login name of the user that logs into the user interface.

display web users

Syntax

display web users

View

Any view

Parameter

None

Description

Use the **display web users** command to display information about web users.

Example

Display information about the current web users.

```
<Sysname> display web users
UserIDName     Language  Level      State    LinkCount LoginTime LastTime
ab820000   admin    Chinese    Management Enable   0        08:41:50  08:45:59
```

Table 1-3 Description on the fields of the **display web users** command

Field	Description
UserID	ID of a web user
Name	Name of the web user
Language	Login language used by the web user
Level	Level of the web user
State	State of the web user
LinkCount	Number of tasks that the web user runs
LoginTime	Time when the web user logged in
LastTime	Last time when the web user accessed the switch

escape-key

Syntax

escape-key { **default** | *character* }

undo escape-key

View

User interface view

Default Level

3: Manage level

Parameters

default: Restores the default escape key combination <Ctrl + C>.

character: Specifies the shortcut key for aborting a task, a single character (or its corresponding ASCII code value in the range 0 to 127) or a string of 1 to 3 characters.

Description

Use the **escape-key** command to define a shortcut key for aborting tasks.

Use the **undo escape-key** command to restore the default shortcut key.

You can use a single character (or its corresponding ASCII code value in the range 0 to 127) or a string of 1 to 3 characters to define a shortcut key. But in fact, only the first character functions as the shortcut key. For example, if you enter an ASCII value 113, the system will use its corresponding character <q> as the shortcut key; if you input the string **q@c**, the system will use the first letter <q> as the shortcut key.

By default, you can use <Ctrl + C> to terminate a task. You can use the **display current-configuration** command to verify the shortcut key you have defined.

Examples

Define <Q> as the escape key.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] escape-key Q
```

To verify the configuration, do the following:

Run the **ping** command to test the connection.

```
<Sysname> ping -c 20 125.241.23.46
  PING 125.241.23.46: 56  data bytes, press Q to break
    Request time out

  --- 125.241.23.46 ping statistics ---
    2 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

Enter <Q>, if the ping task is terminated and return to the current view, the configuration is correct.

```
<Sysname>
```

flow-control

Syntax

flow-control { **hardware** | **none** | **software** }

undo flow-control

View

AUX interface view

Default Level

2: System level

Parameters

hardware: Configures to perform hardware flow control.

none: Configures no flow control.

software: Configures to perform software flow control.

Description

Using **flow-control** command, you can configure the flow control mode on AUX port. Using **undo flow-control** command, you can restore the default flow control mode.

By default, the value is **none**. That is, no flow control will be performed.

Note

Switch 4210G only support **none** keyword.

Examples

Configure software flow control on AUX port.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] flow-control none
```

free user-interface

Syntax

free user-interface [*type*] *number*

View

User view

Default Level

3: Manage level

Parameters

type: User interface type.

number: Absolute user interface index or relative user interface index.

- Relative user interface index: If you provide the *type* argument, *number* indicates the user interface index of the type. When the type is AUX, the *number* is 0; when the type is VTY, the *number* ranges from 0 to 4.
- Absolute user interface index: If you do not provide the *type* argument, *number* indicates absolute user interface index, which ranges from 0 to 5.

Description

Use the **free user-interface** command to clear a specified user interface. If you execute this command, the corresponding user interface will be disconnected.

Note that the current user interface can not be cleared.

Examples

Log into user interface 0 and clear user interface 1.

```
<Sysname> free user-interface 1
Are you sure to free user-interface vty0
[Y/N]y
[OK]
```

After you execute this command, user interface 1 will be disconnected. The user in it must log in again to connect to the switch.

history-command max-size

Syntax

history-command max-size *value*

undo history-command max-size

View

User interface view

Default Level

2: System level

Parameters

value: Size of the history command buffer. This argument ranges from 0 to 256 and defaults to 10. That is, the history command buffer can store 10 commands by default.

Description

Use the **history-command max-size** command to set the size of the history command buffer.

Use the **undo history-command max-size** command to revert to the default history command buffer size.

Examples

Set the size of the history command buffer to 20 to enable it to store up to 20 commands.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] history-command max-size 20
```

idle-timeout

Syntax

idle-timeout *minutes* [*seconds*]

undo idle-timeout

View

User interface view

Default Level

2: System level

Parameters

minutes: Number of minutes. This argument ranges from 0 to 35,791.

seconds: Number of seconds. This argument ranges from 0 to 59.

Description

Use the **idle-timeout** command to set the timeout time. The connection to a user interface is terminated if no operation is performed in the user interface within the specified period.

Use the **undo idle-timeout** command to revert to the default timeout time.

You can use the **idle-timeout** 0 command to disable the timeout function.

The default timeout time is 10 minutes.

Examples

Set the timeout time of AUX 0 to 1 minute.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] idle-timeout 1 0
```

lock

Syntax

lock

View

User view

Default Level

3: Manage level

Parameters

None

Description

Use the **lock** command to lock the current user interface to prevent unauthorized users from operating the user interface.

With the execution of this command, the system prompts to enter and confirm the password (up to 16 characters), and then locks the user interface.

To cancel the lock, press the **Enter** key and enter the correct password.

By default, the system will not lock the current user interface automatically.

Examples

Lock the current user interface.

```
<Sysname> lock
Please input password<1 to 16> to lock current user terminal interface:
Password:
Again:


                locked !
```

Cancel the lock.

```
Password:
Again:
<Sysname>
```

parity

Syntax

parity { **even** | **mark** | **none** | **odd** | **space** }

undo parity

View

AUX interface view

Default Level

2: System level

Parameters

even: Performs even checks.

mark: Performs mark checks.

none: Does not check.

odd: Performs odd checks.

space: Performs space checks.

Description

Use the **parity** command to set the check mode of the user interface.

Use the **undo parity** command to revert to the default check mode.

No check is performed by default.

 **Note**

3COM switch 4210G support the **even**, **none**, and **odd** check modes only. To establish the connection again, you need to modify the configuration of the termination emulation utility running on your PC accordingly.

Examples

Set to perform mark checks.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] parity mark
```

protocol inbound

Syntax

protocol inbound { **all** | **ssh** | **telnet** }

View

VTY interface view

Default Level

3: Manage level

Parameters

all: Supports both Telnet protocol and SSH protocol.

ssh: Supports SSH protocol.

telnet: Supports Telnet protocol.

Description

Use the **protocol inbound** command to configure the user interface to support specified protocols.

Both Telnet and SSH protocols are supported by default.

Related command: **user-interface vty**.

Caution

If you want to configure the user interface to support SSH, to ensure a successful login, you must first configure the authentication mode to **scheme** on the user interface. If you set the authentication mode to **password** or **none**, the **protocol inbound ssh** command will fail. Refer to authentication-mode.

Examples

Configure VTY 0 to support only SSH protocol.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] protocol inbound ssh
```

screen-length

Syntax

screen-length *screen-length*

undo screen-length

View

User interface view

Default Level

2: System level

Parameters

screen-length: Number of lines the screen can contain. This argument ranges from 0 to 512 and defaults to 24.

Description

Use the **screen-length** command to set the number of lines the terminal screen can contain.

Use the **undo screen-length** command to revert to the default number of lines.

You can use the **screen-length** 0 command to disable the function to display information in pages.

Examples

Set the number of lines the terminal screen can contain to 20.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] screen-length 20
```

send

Syntax

send { **all** | *number* | *type number* }

View

User view

Default Level

1: Monitor level

Parameters

all: Specifies to send messages to all user interfaces.

type: User interface type.

number: Absolute user interface index or relative user interface index.

- Relative user interface index: If you provide the *type* argument, the *number* argument indicates the user interface index of the type. When the type is AUX, *number* is from 0 to 3; when the type is VTY, *number* ranges from 0 to 4.
- Absolute user interface index: If you do not provide the *type* argument, the *number* argument indicates the absolute user interface index, and ranges from 0 to 13.

Description

Use the **send** command to send messages to a specified user interface or all user interfaces.

Examples

Send messages to all user interfaces.

```
<Sysname> send all
Enter message, end with CTRL+Z or Enter; abort with CTRL+C:
hello^Z
Send message? [Y/N]y
<Sysname>

***
***
***Message from vty0 to vty0
***
hello

<Sysname>
```

set authentication password

Syntax

set authentication password { **cipher** | **simple** } *password*

undo set authentication password

View

User interface view

Default Level

3: Manage level

Parameters

cipher: Specifies to display the local password in encrypted text when you display the current configuration.

simple: Specifies to display the local password in plain text when you display the current configuration.

password: Password. The password must be in plain text if you specify the **simple** keyword in the **set authentication password** command. If you specify the **cipher** keyword, the password can be in either encrypted text or plain text. Whether the password is in encrypted text or plain text depends on the password string entered. Strings containing up to 16 characters (such as 123) are regarded as plain text passwords and are converted to the corresponding 24-character encrypted password (such as !TP<*EMUHL,408`W7TH!Q!!). A encrypted password must contain 24 characters and must be in ciphered text (such as !TP<\*EMUHL,408`W7TH!Q!!).

Description

Use the **set authentication password** command to set the local password.

Use the **undo set authentication password** command to remove the local password.

Note that only plain text passwords are expected when users are authenticated.

Note

By default, Telnet users need to provide their passwords to log in. If no password is set, the “Login password has not been set !” message appears on the terminal when users log in.

Examples

Set the local password of VTY 0 to “123”.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] set authentication password simple 123
```

shell

Syntax

shell

undo shell

View

User interface view

Default Level

3: Manage level

Parameters

None

Description

Use the **shell** command to make terminal services available for the user interface.

Use the **undo shell** command to make terminal services unavailable to the user interface.

By default, terminal services are available in all user interfaces.

Note the following when using the **undo shell** command:

- This command is available in all user interfaces except the AUX user interface, because the AUX port (also the Console) is exclusively used for configuring the switch.
- This command is unavailable in the current user interface.
- This command prompts for confirmation when being executed in any valid user interface.

Examples

Log into user interface 0 and make terminal services unavailable in VTY 0 through VTY 4.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] undo shell
```

```
% Disable ui-vty0-4 , are you sure ? [Y/N]y
```

speed

Syntax

speed *speed-value*

undo speed

View

AUX interface view

Default Level

2: System level

Parameters

speed-value: Transmission speed (in bps). This argument can be 300, 600, 1200, 2400, 4800, 9600, 19,200, 38,400, 57,600, 115,200 and defaults to 19,200.

Description

Use the **speed** command to set the transmission speed of the user interface.

Use the **undo speed** command to revert to the default transmission speed.

 **Note**

After you use the **speed** command to configure the transmission speed of the AUX user interface, you must change the corresponding configuration of the terminal emulation program running on the PC, to keep the configuration consistent with that on the switch.

Examples

Set the transmission speed of the AUX user interface to 9600 bps.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] speed 9600
```

stopbits

Syntax

stopbits { **1** | **1.5** | **2** }

undo stopbits

View

AUX interface view

Default Level

2: System level

Parameters

1: Sets the stop bits to 1.

1.5: Sets the stop bits to 1.5.

2: Sets the stop bits to 2.

Description

Use the **stopbits** command to set the stop bits of the user interface.

Use the **undo stopbits** command to revert to the default stop bits.

By default, the stop bits is 1.

Note

- The switch 4210G do not support communication with a terminal emulation program with stopbits set to 1.5.
- Changing the stop bits value of the switch to a value different from that of the terminal emulation utility does not affect the communication between them.

Examples

Set the stop bits to 2.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface aux 0
[Sysname-ui-aux0] stopbits 2
```

sysname

Syntax

sysname *string*

undo sysname

View

System view

Default Level

2: System level

Parameters

string: System name of the switch. This argument can contain 1 to 30 characters and defaults to **4210G**.

Description

Use the **sysname** command to set a system name for the switch.

Use the **undo sysname** command to revert to the default system name.

The CLI prompt reflects the system name of a switch. For example, if the system name of a switch is “4210G”, then the prompt of user view is <4210G >.

Examples

Set the system name of the switch to **ABC**.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] sysname ABC
[ABC]
```

telnet

Syntax

telnet *remote-system* [*port-number*] [**source** { **ip** *ip-address* | **interface** *interface-type interface-number* }]

View

User view

Default Level

0: Visit level

Parameters

remote-system: IP address or host name of the remote system. The host name is a string of 1 to 20 characters, which can be specified using the **ip host** command.

port-number: TCP port number assigned to Telnet service on the remote system, in the range 0 to 65535.

ip-address: Source IP address of the packets sent by the Telnet client.

interface-type interface-number: Type and number of the interface through which the Telnet client sends packets.

Description

Use the **telnet** command to Telnet to another switch from the current switch to manage the former remotely. You can terminate a Telnet connection by pressing <Ctrl + K>.

Related commands: **display tcp status, ip host**.

Examples

Telnet to the switch with the host name of **Sysname2** and IP address of 129.102.0.1 from the current switch (with the host name of **Sysname1**).

```
<Sysname1> telnet 129.102.0.1
Trying 129.102.0.1 ...
Press CTRL+K to abort
```

```
Connected to 129.102.0.1 ...
******************************************************************************
* Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved. *
* This software is protected by copyright law and international treaties.    *
* Without the prior written permission of 3Com Corporation and its licensors,*
* any reproduction republication, redistribution, decompiling, reverse       *
* engineering is strictly prohibited. Any unauthorized use of this software  *
* or any portion of it may result in severe civil and criminal penalties, and*
* will be prosecuted to the maximum extent possible under the applicable law.*
******************************************************************************

<Sysname2>
```

telnet ipv6

Syntax

telnet ipv6 *remote-system* [**-i** *interface-type interface-number*] [*port-number*]

View

User view

Default Level

0: Visit level

Parameters

remote-system: IPv6 address or host name of the remote system. An IPv6 address can be up to 46 characters; a host name is a string of 1 to 20 characters.

-i *interface-type interface-number*: Specifies the outbound interface by interface type and interface number. The outbound interface is required when the destination address is a local link address.

port-number: TCP port number assigned to Telnet service on the remote system, in the range 0 to 65535 and defaults to 23.

Description

Use the **telnet ipv6** command to telnet to a remote device for remote management. You can terminate a Telnet connection by pressing <Ctrl + K>.

Examples

Telnet to the device with IPv6 address 3001::1.

```
<Sysname> telnet ipv6 3001::1
Trying 3001::1 ...
Press CTRL+K to abort
Connected to 3001::1 ...
******************************************************************************
* Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved. *
* This software is protected by copyright law and international treaties.    *
* Without the prior written permission of 3Com Corporation and its licensors,*
* any reproduction republication, redistribution, decompiling, reverse       *
```

```
* engineering is strictly prohibited. Any unauthorized use of this software  *
* or any portion of it may result in severe civil and criminal penalties, and*
* will be prosecuted to the maximum extent possible under the applicable law.*
**************************************************************************

<Sysname>
```

telnet client source

Syntax

telnet client source { **ip** *ip-address* | **interface** *interface-type interface-number* }

undo telnet client source

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **telnet client source** command to specify the source IP address or source interface for the Telnet packets to be sent.

Use the **undo telnet client source** command to remove the source IP address or source interface configured for Telnet packets.

By default, source IP address or source interface of the Telnet packets sent is not configured.

Examples

Specify the source IP address for Telnet packets.

```
<Sysname> system-view
[Sysname] telnet client source ip 129.102.0.2
```

Remove the source IP address configured for Telnet packets.

```
[Sysname] undo telnet client source
```

telnet server enable

Syntax

telnet server enable

undo telnet server enable

View

System view

Default Level

3: Manage level

Parameters

None

Description

Use the **telnet server enable** command to make the switch to operate as a Telnet Server.

Use the **undo telnet server enable** command disable the switch from operating as a Telnet server.

By default, a switch does not operate as a Telnet server.

Examples

Make the switch to operate as a Telnet Server.

```
<Sysname> system-view
[Sysname] telnet server enable
% Start Telnet server
```

Disable the switch from operating as a Telnet server.

```
[Sysname] undo telnet server enable
% Close Telnet server
```

terminal type

Syntax

terminal type { **ansi** | **vt100** }

undo terminal type

View

User interface view

Default Level

2: System level

Parameters

ansi: Specifies the terminal display type to ANSI.

vt100: Specifies the terminal display type to VT100.

Description

Use the **terminal type** command to configure the type of terminal display .

Use the **undo terminal type** command to restore the default.

Currently, the system support two types of terminal display : ANSI and VT100.

By default, the terminal display type is ANSI. The device must use the same display type as the terminal. If the terminal uses VT 100, the device should also use VT 100.

Examples

Set the terminal display type to VTY 100.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] terminal type vt100
```

user-interface

Syntax

user-interface [*type*] *first-number* [*last-number*]

View

System view

Default Level

2: System level

Parameters

type: User interface type.

first-number: User interface index, which identifies the first user interface to be configured.

last-number: User interface index, which identifies the last user interface to be configured.

Description

Use the **user-interface** command to enter one or more user interface views to perform configuration.

Examples

Enter VTY 0 user interface view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0]
```

user privilege level

Syntax

user privilege level *level*

undo user privilege level

View

User interface view

Default Level

3: Manage level

Parameters

level: Command level ranging from 0 to 3.

Description

Use the **user privilege level** command to configure the command level available to the users logging into the user interface.

Use the **undo user privilege level** command to revert to the default command level.

By default, the commands of level 3 are available to the users logging into the AUX user interface. The commands of level 0 are available to the users logging into VTY user interfaces.

Commands fall into four command levels: visit, monitor, system, and manage, which are described as follows:

- Visit level: Commands of this level are used to diagnose network and change the language mode of user interface, such as the **ping**, **tracert**. The **Telnet** command is also of this level. Commands of this level cannot be saved in configuration files.
- Monitor level: Commands of this level are used to maintain the system, to debug service problems, and so on. The **display** and **debugging** command are of monitor level. Commands of this level cannot be saved in configuration files.
- System level: Commands of this level are used to configure services. Commands concerning routing and network layers are of system level. You can utilize network services by using these commands.
- Manage level: Commands of this level are for the operation of the entire system and the system supporting modules. Services are supported by these commands. Commands concerning file system, file transfer protocol (FTP), trivial file transfer protocol (TFTP), downloading using XModem, user management, and level setting are of administration level.

Examples

Configure that commands of level 0 are available to the users logging into VTY 0.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0
[Sysname-ui-vty0] user privilege level 0
```

You can verify the above configuration by Telnetting to VTY 0 and displaying the available commands, as listed in the following.

```
<Sysname> ?
User view commands:
  ping             Ping function
  quit             Exit from current command view
  super            Set the current user priority level
  telnet           Establish one TELNET connection
  tracert          Trace route function
  undo             Undo a command or set to its default status
```

2 Commands for Controlling Login Users

Commands for Controlling Login Users

acl

Syntax

acl [**ipv6**] *acl-number* { **inbound** | **outbound** }

undo acl [**ipv6**] { **inbound** | **outbound** }

View

User interface view

Default Level

2: System level

Parameters

acl-number: ACL number ranging from 2000 to 4999, where:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Layer 2 ACLs

ipv6 *acl-number*: IPv6 ACL number ranging from 2000 to 3999.

inbound: Filters the users Telnetting to the current switch.

outbound: Filters the users Telnetting to other switches from the current switch.

Description

Use the **acl** command to apply an ACL to filter Telnet users.

Use the **undo acl** command to disable the switch from filtering Telnet users using the ACL.

Note that if you use Layer 2 ACL rules, you can only choose the **inbound** keyword in the command here.

Examples

Apply ACL 2000 to filter users Telnetting to the current switch (assuming that ACL 2,000 already exists.)

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] acl 2000 inbound
```

free web-users

Syntax

free web-users { **all** | **user-id** *userid* | **user-name** *username* }

View

User view

Parameter

userid: Web user ID.

username: User name of the Web user. This argument can contain 1 to 80 characters.

all: Specifies all Web users.

Description

Use the **free web-users** command to disconnect a specified Web user or all Web users by force.

Example

Disconnect all Web users by force.

```
<Sysname> free web-users all
```

3 Basic System Configuration Commands

Basic System Configuration Commands

clock datetime

Syntax

clock datetime *time date*

View

User view

Default Level

3: Manage level

Parameters

time: Current time in the format of *HH:MM:SS*, where *HH* is hours in the range 0 to 23, *MM* is minutes in the range 0 to 59, and *SS* is seconds in the range 0 to 59. The zeros in the argument can be omitted except for indicating 0 hours.

date: Current date in the format of *MM/DD/YYYY* or *YYYY/MM/DD*. *MM* is the month of the year in the range 1 to 12, *DD* is the day of the month that varies with months, and *YYYY* is a year in the range 2000 to 2035.

Description

Use the **clock datetime** command to set the current time and date of the device.

The current time and date of the device must be set in an environment that requires the acquisition of absolute time.

You may choose not to provide seconds when inputting the time parameters.

Related commands: **clock summer-time one-off**, **clock summer-time repeating**, **clock timezone**, **display clock**.

Examples

Set the current system time to 14:10:20 08/01/2005.

```
<Sysname> clock datetime 14:10:20 8/1/2005
```

Set the current system time to 00:06:00 01/01/2007.

```
<Sysname> clock datetime 0:6 2007/1/1
```

clock summer-time one-off

Syntax

clock summer-time *zone-name* **one-off** *start-time start-date end-time end-date add-time*

undo clock summer-time

View

System view

Default Level

3: Manage level

Parameters

zone-name: Name of the daylight saving time, a string of 1 to 32 characters. It is case sensitive.

start-time: Start time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

start-date: Start date, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.

end-time: End time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

end-date: End date, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.

add-time: Time added to the standard time of the device, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

Description

Use the **clock summer-time one-off** command to adopt daylight saving time from the *start-time* of the *start-date* to the *end-time* of the *end-date*. Daylight saving time adds the *add-time* to the current time of the device.

Use the **undo clock summer-time** command to cancel the configuration of the daylight saving time.

After the configuration takes effect, you can use the **display clock** command to view it. Besides, the time of the log or debug information is the local time of which the time zone and daylight saving time have been adjusted.

Note that:

- The time range from *start-time* in *start-date* to *end-time* in *end-date* must be longer than one day and shorter than one year. Otherwise, the argument is considered as invalid and the configuration fails.
- If the current system time is in the time range specified with this command, the system time automatically adds “add-time” after the execution of this command.

Related commands: **clock datetime**, **clock summer-time repeating**, **clock timezone**, **display clock**.

Examples

For daylight saving time in **abc1** between 06:00:00 on 08/01/2006 and 06:00:00 on 09/01/2006, set the system clock ahead one hour.

```
<Sysname> system-view
[Sysname] clock summer-time abc1 one-off 6 08/01/2006 6 09/01/2006 1
```

clock summer-time repeating

Syntax

clock summer-time *zone-name* **repeating** *start-time start-date end-time end-date add-time*

undo clock summer-time

View

System view

Default Level

3: Manage level

Parameters

zone-name: Name of the daylight saving time, a string of 1 to 32 characters.

start-time: Start time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

start-date: Start date which can be set in two ways:

- Enter the year, month and date at one time, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.
- Enter the year, month and date one by one, separated by spaces. The year ranges from 2000 to 2035; the month can be **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**; the start week can be the **first**, **second**, **third**, **fourth**, **fifth** or **last** week of the month; the start date is **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**.

end-time: End time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

end-date: End date which can be set in two ways:

- Enter the year, month and date at one time, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.
- Enter the year, month and date one by one, separated by spaces. The year ranges from 2000 to 2035; the month can be **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**; the end week can be the **first**, **second**, **third**, **fourth**, **fifth** or **last** week of the month; the end date is **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**.

add-time: Time added to the current standard time of the device, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

Description

Use the **clock summer-time repeating** command to adopt summer-time repeatedly.

Use the **undo clock summer-time** command to cancel the configuration of the daylight saving time.

For example, when *start-date* and *start-time* are set to 2007/6/6 and 00:00:00, *end-date* and *end-time* to 2007/10/01 and 00:00:00, and *add-time* to 01:00:00, it specifies to adopt daylight saving time from 00:00:00 of June 6 until 00:00:00 of October 1 each year from 2007 (2007 inclusive). The daylight saving time adds one hour to the current device time.

After the configuration takes effect, use the **display clock** command to view the result. The information such as log file and debug adopts the local time modified by time-zone and daylight saving time.

Note that:

- The time range from “start-time” in “start-date” to “end-time” in “end-date” must be longer than one day and shorter than one year. Otherwise, the argument is considered as invalid and the configuration fails.
- If the current system time is in the time range specified with this command, the system time automatically adds “add-time” after the execution of this command.

Related commands: **clock datetime**, **clock summer-time one-off**, **clock timezone**, **display clock**.

Examples

For the daylight saving time in **abc2** between 06:00:00 on 08/01/2007 and 06:00:00 on 09/01/2007 and from 06:00:00 08/01 to 06:00:00 on 09/01 each year after 2007, set the system clock ahead one hour.

```
<Sysname> system-view
[Sysname] clock summer-time abc2 repeating 06:00:00 08/01/2007 06:00:00 09/01/2007 01:00:00
```

clock timezone

Syntax

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

undo clock timezone

View

System view

Default Level

3: Manage level

Parameters

zone-name: Time zone name, a string of 1 to 32 characters. It is case sensitive.

add: Positive offset to universal time coordinated (UTC) time.

minus: Negative offset to UTC time.

zone-offset: Offset to UTC time. In the format of *HH/MM/SS* (hours/minutes/seconds), where *HH* is hours in the range 0 to 23, *MM* is minutes in the range 0 to 59, and *SS* is seconds in the range 0 to 59. The zeros in the argument can be omitted except for indicating 0 hours.

Description

Use the **clock timezone** command to set the local time zone.

Use the **undo clock timezone** command to restore the local time zone to the default UTC time zone.

By default, the local time zone is UTC zone.

After the configuration takes effect, use the **display clock** command to view the result. The information such as log file and debug adopts the local time modified by time-zone and daylight saving time.

Related commands: **clock datetime**, **clock summer-time one-off**, **clock summer-time repeating**, **display clock**.

Examples

Set the name of the local time zone to **Z5**, five hours ahead of UTC time.

```
<Sysname> system-view
[Sysname] clock timezone z5 add 5
```

command-alias enable

Syntax

command-alias enable

undo command-alias enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **command-alias enable** command to enable the command alias function.

Use the **undo command-alias enable** command to disable the command alias function.

By default, the command alias function is disabled, that is, you cannot configure command aliases.

Examples

Enable the command alias function.

```
<Sysname> system-view
[Sysname] command-alias enable
```

Disable the command alias function.

```
<Sysname> system-view
[Sysname] undo command-alias enable
```

command-alias mapping

Syntax

command-alias mapping *cmdkey alias*

undo command-alias mapping *cmdkey*

View

System view

Default Level

2: System level

Parameters

cmdkey: The complete form of the first keyword of a command for which an alias will be configured.

alias: Specifies the command alias, which cannot be the same with the first keyword of an existing command.

Description

Use the **command-alias mapping** command to configure command aliases.

Use the **undo command-alias mapping** command to delete command aliases.

By default, a command has no alias.

Examples

Configure command aliases by specifying **show** as the replacement of the **display** keyword.

```
<Sysname> system-view
[Sysname] command-alias mapping display show
```

After the above configuration, the **display** commands have their aliases. For example, if the original command is **display clock**, now its alias is **show clock** and you can input the alias to view the system time and date.

Delete the command aliases by canceling the replacement of the **display** keyword.

```
<Sysname> system-view
[Sysname] undo command-alias mapping display
```

command-privilege level

Syntax

command-privilege level *level* **view** *view command*

undo command-privilege view *view command*

View

System view

Default Level

3: Manage level

Parameters

level *level*: Command level, in the range 0 to 3.

view *view*: Specifies a view. The value **shell** of the argument *view* represents user view. The specified view must be the view to which the command provided by the *command* argument belongs; for the corresponding view, refer to the "View" section of the specified command.

command: Command to be set in the specified view.

Description

Use the **command-privilege** command to assign a level for the specified command in the specified view.

Use the **undo command-privilege view** command to restore the default.

By default, each command in a view has its specified level. For the details, refer to the related part of *Basic System Configuration* in this manual. Command level falls into four levels: visit, monitor, system, and manage, which are identified by 0 through 3. The administrator can assign a privilege level for a user according to his need. When the user logs on a device, the commands available depend on the user's privilege. For example, if a user's privilege is 3 and the command privilege of VTY 0 user interface is 1, and the user logs on the system from VTY 0, he can use all the commands with privilege smaller than three (inclusive).

Note that:

- You are recommended to use the default command level or modify the command level under the guidance of professional staff; otherwise, the change of command level may bring inconvenience to your maintenance and operation, or even potential security problem.
- When you configure the **command-privilege** command, the value of the *command* argument must be a complete form of the specified command, that is, you must enter all needed keywords and arguments of the command. The argument should be in the value range. For example, the default level of the **tftp** *server-address* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] command is 3; after the **command-privilege level** 0 **view** shell tftp 1.1.1.1 put a.cfg command is executed, when users with the user privilege level of 0 log in to the device, they can execute the **tftp** *server-address* **put** *source-filename* command (such as the **tftp** 192.168.1.26 **put** syslog.txt command); users with the user privilege level of 0 cannot execute the command with the **get**, **sget** or **source** keyword, and cannot specify the *destination-filename* argument.
- When you configure the **undo command-privilege view** command, the value of the *command* argument can be an abbreviated form of the specified command, that is, you only need to enter the keywords at the beginning of the command. For example, after the **undo command-privilege view** system ftp command is executed, all commands starting with the keyword **ftp** (such as **ftp server acl**, **ftp server enable**, and **ftp timeout**) will be restored to the default level; if you have modified the command level of commands **ftp server enable** and **ftp timeout**, and you want to restore only the **ftp server enable** command to its default level, you should use the **undo command-privilege view** system ftp server command.
- If you modify the command level of a command in a specified view from the default command level to a lower level, remember to modify the command levels of the **quit** command and the corresponding command that is used to enter this view. For example, the default command level of commands **interface** and **system-view** is 2 (system level); if you want to make the **interface** command available to the users with the user privilege level of 1, you need to execute the following three commands: **command-privilege level** 1 **view** shell system-view, **command-privilege level** 1 **view** system interface gigabitethernet 1/0/1, and **command-privilege level** 1 **view** system quit, so that the login users with the user privilege level of 1 can enter system view, execute the **interface gigabitethernet** command, and then return to user view.

Examples

Set the command level of the **system-view** command in user view to 3. (By default, users with the user privilege level of 2 or 3 can use the **system-view** command after login; after the following configuration, only users with the user privilege level of 3 can use this command to enter system view and configure the device. Therefore, the device security is improved.)

```
<Sysname> system-view
[Sysname] command-privilege level 3 view shell system-view
```

copyright-info enable

Syntax

copyright-info enable

undo copyright-info enable

View

System view

Default Level

3: Manage level

Parameters

None

Description

Use the **copyright-info enable** command to enable the display of copyright information.

Use the **undo copyright-info enable** command to disable the display of copyright information.

By default, the display of copyright information is enabled.

Examples

Enable the display of copyright information

```
<Sysname> system-view
[Sysname] copyright-info enable
```

- If a user logs in to the device through Telnet, the following information is displayed:

```
******************************************************************************
* Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved. *
* This software is protected by copyright law and international treaties.    *
* Without the prior written permission of 3Com Corporation and its licensors,*
* any reproduction republication, redistribution, decompiling, reverse       *
* engineering is strictly prohibited. Any unauthorized use of this software  *
* or any portion of it may result in severe civil and criminal penalties, and*
* will be prosecuted to the maximum extent possible under the applicable law.*
******************************************************************************

<Sysname>
```

- If a user has already logged in through the console port, and then quits user view, the following information is displayed:

```
******************************************************************************
* Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved. *
* This software is protected by copyright law and international treaties.    *
* Without the prior written permission of 3Com Corporation and its licensors,*
* any reproduction republication, redistribution, decompiling, reverse       *
* engineering is strictly prohibited. Any unauthorized use of this software  *
* or any portion of it may result in severe civil and criminal penalties, and*
* will be prosecuted to the maximum extent possible under the applicable law.*
******************************************************************************
```

```
User interface aux0 is available.



Please press ENTER.
```

display clipboard

Syntax

display clipboard

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display clipboard** command to view the contents of the clipboard.

To copy the specified content to the clipboard:

Move the cursor to the starting position of the content and press the <Esc+Shift+,> combination (“,” is an English comma).

Move the cursor to the ending position of the content and press the <Esc+Shift+.> combination (“.” is an English dot) to copy the specified content to the clipboard.

Examples

View the content of the clipboard.

```
<Sysname> display clipboard
---------------- CLIPBOARD-----------------
       display arp all
```

display clock

Syntax

display clock

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display clock** command to view the current system time and date.

The current system time and date are decided by the **clock datetime**, **clock summer-time one-off** (or **clock summer-time repeating**), **clock timezone**. Refer to *Configuring the system clock* in the operation manual for the detailed rules.

Related commands: **clock datetime**, **clock summer-time one-off**, **clock summer-time repeating**, **clock timezone**.

Examples

Display the current time and date.

```
<Sysname> display clock
09:41:23 UTC Thu 12/15/2005
```

display command-alias

Syntax

display command-alias

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display configure-user** command to display defined command aliases and the corresponding commands.

Examples

Display the defined command aliases and the corresponding commands.

```
<Sysname> display command-alias
Command alias is enabled
index  alias                    command key
1      show                     display
```

display current-configuration

Syntax

display current-configuration [[**configuration** [*configuration*] | **interface** [*interface-type*] [*interface-number*]] [**by-linenum**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]]

View

Any view

Default Level

2: System level

Parameters

configuration [*configuration*]: Specifies to display non-interface configuration. If no parameter is used, all the non-interface configuration is displayed; if parameters are used, display the specified information. For example:

- **isp**: Displays the ISP configuration.
- **ospf**: Displays the ospf configuration.
- **radius-template**: Displays the Radius template configuration.
- **system**: Displays the system configuration.
- **user-interface**: Displays the user interface configuration.

interface [*interface-type*] [*interface-number*]: Displays the interface configuration, where *interface-type* represents the interface type and *interface-number* represents the interface number.

by-linenum: Specifies to display the number of each line.

|: Specifies to use regular expression to filter the configuration of display device. For the detailed description of the regular expression, refer to the *CLI Display* part of *Basic System Configuration* in the *System Volume*.

- **begin**: Displays the line that matches the regular expression and all the subsequent lines.
- **exclude**: Displays the lines that do not match the regular expression.
- **include**: Displays only the lines that match the regular expression.

regular-expression: Regular expression, a string of 1 to 256 characters. Note that this argument is case-sensitive and can have spaces included.

Description

Use the **display current-configuration** command to display the current validated configuration of a device.

You can use the **display current-configuration** command to view the currently validated configuration. A parameter is not displayed if it has the default configuration. If the validated parameter is changed, although you have configured it, the validated parameter is displayed. For example, ip address 11.11.11.11 24 has been configured on a Loopback interface. In this case, if you execute the **display current-configuration** command, ip address 11.11.11.11 255.255.255.255 is displayed, meaning the validated subnet mask is 32 bits.

Related commands: **save**, **reset saved-configuration**, **display saved-configuration**.

Examples

Display the configuration from the line containing “user-interface” to the last line in the current validated configuration (the output information depends on the current configuration).

```
<Sysname> display current-configuration | begin user-interface
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
```

```
 user privilege level 3
#
return
```

display default-configuration

Syntax

display default-configuration

View

Any view

Default Level

2: System level

Parameters

None

Description

Use the **display default-configuration** command to display the factory defaults of a device. The command displays all commands to be executed when the device boots with the factory defaults.

Related commands: **display current-configuration**, **display saved-configuration**.

Examples

Display the factory defaults of the device (The factory defaults vary with device models. The detailed displays are omitted here).

```
<Sysname> display default-configuration
```

display diagnostic-information

Syntax

display diagnostic-information

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display diagnostic-information** command to display or save the statistics of each module's running status in the system.

When the system is out of order, you need to collect a lot of information to locate the problem. At this time you can use the **display diagnostic-information** command to display or save the statistics of

each module's running status in the system. The **display diagnostic-information** command collects prompt information of the commands **display clock**, **display version**, **display device**, and **display current-configuration**.

Examples

Save the statistics of each module's running status in the system.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)?[Y/N]y
Please input the file name(*.diag)[flash:/default.diag]:aa.diag
Diagnostic information is outputting to flash:/aa.diag.
Please wait...
Save succeeded.
```

You can view the content of the file aa.diag by executing the **more aa.diag** command in user view, in combination of the **Page Up** and **Page Down** keys.

Display the statistics of each module's running status in the system.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:n
```

display history-command

Syntax

display history-command

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display history-command** command to display commands saved in the history buffer.

The system will save validated history commands performed last in current user view to the history buffer, which can save up to ten commands by default. You can use the **history-command max-size** command to set the size of the history buffer. Refer to the **history-command max-size** command in *Login Commands* in the *System Volume* for related configuration.

Examples

Display validated history commands in current user view (the display information varies with configuration).

```
<Sysname> display history-command
  display history-command
  system-view
  vlan 2
```

```
quit
```

display hotkey

Syntax

display hotkey

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display hotkey** command to display hotkey information.

Examples

Display hotkey information.

```
<Sysname> display hotkey
----------------- HOTKEY -----------------

          =Defined hotkeys=
Hotkeys Command
CTRL_G  display current-configuration
CTRL_L  display ip routing-table
CTRL_O  undo debug all

         =Undefined hotkeys=
Hotkeys Command
CTRL_T  NULL
CTRL_U  NULL

          =System hotkeys=
Hotkeys Function
CTRL_A  Move the cursor to the beginning of the current line.
CTRL_B  Move the cursor one character left.
CTRL_C  Stop current command function.
CTRL_D  Erase current character.
CTRL_E  Move the cursor to the end of the current line.
CTRL_F  Move the cursor one character right.
CTRL_H  Erase the character left of the cursor.
CTRL_K  Kill outgoing connection.
CTRL_N  Display the next command from the history buffer.
CTRL_P  Display the previous command from the history buffer.
CTRL_R  Redisplay the current line.
```

```
CTRL_V  Paste text from the clipboard.
CTRL_W  Delete the word left of the cursor.
CTRL_X  Delete all characters up to the cursor.
CTRL_Y  Delete all characters after the cursor.
CTRL_Z  Return to the User View.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor one word back.
ESC_D   Delete remainder of word.
ESC_F   Move the cursor forward one word.
ESC_N   Move the cursor down a line.
ESC_P   Move the cursor up a line.
ESC_<   Specify the beginning of clipboard.
ESC_>   Specify the end of clipboard.
```

display this

Syntax

display this [**by-linenum**]

View

Any view

Default Level

1: Monitor level

Parameters

by-linenum: Specifies to display the number of each line.

Description

Use the **display this** command to display the validated configuration under the current view.

After finishing a set of configurations under a view, you can use the **display this** command to check whether the configuration takes effect.

Note that:

- A parameter is not displayed if it has the default configuration.
- A parameter is not displayed if the configuration has not taken effect.
- When you use the command in a user interface view, the command displays the valid configuration in all the user interfaces.
- When you use the command in a VLAN view, the command displays configurations of all created VLANs.

Examples

Display the valid configuration information of the current view (the output information depends on the current configuration of the device).

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] display this
#
```

```
user-interface aux 0
user-interface vty 0
 history-command max-size 256
user-interface vty 1 4
#
return
```

display version

Syntax

display version

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display version** command to view system version information.

By viewing system version information, you can learn about the current software version, rack type and the information related to the interface boards.

Examples

Display system version information (The system version information varies with devices.).

```
<Sysname> display version
```

header

Syntax

header { **incoming** | **legal** | **login | motd** | **shell** } *text*

undo header { **incoming** | **legal** | **login** | **motd** | **shell** }

View

System view

Default Level

2: System level

Parameters

incoming: Sets the banner displayed when a Modem login user enters user view. If authentication is needed, the incoming banner is displayed after the authentication is passed.

legal: Sets the authorization banner before a user logs onto the terminal interface. The legal banner is displayed before the user inputs the username and password.

login: Sets the login banner at authentication.

motd: Banner displayed before login. If authentication is required, the banner is displayed before authentication.

shell: Sets the banner displayed when a non Modem login user enters user view.

text: Banner message, which can be input in two formats. Refer to *Basic System Configuration* for the detailed information.

Description

Use the **header** command to create a banner.

Use the **undo header** command to clear a banner.

Examples

```
# Configure banners.<Sysname> system-view
[Sysname] header incoming %
Please input banner content, and quit with the character '%'.
Welcome to incoming(header incoming)%
[Sysname] header legal %
Please input banner content, and quit with the character '%'.
Welcome to legal (header legal)%
[Sysname] header login %
Please input banner content, and quit with the character '%'.
Welcome to login(header login)%
[Sysname] header motd %
Please input banner content, and quit with the character '%'.
Welcome to motd(header motd)%
[Sysname] header shell %
Please input banner content, and quit with the character '%'.
Welcome to shell(header shell)%
```

Note

The character % is the starting/ending character of text in this example. Entering % after the displayed text quits the **header** command.

As the starting and ending character, % is not a part of a banner.

```
# Test the configuration remotely using Telnet. (only when login authentication is configured
can the login banner be displayed).
**************************************************************************
* Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved. *
* This software is protected by copyright law and international treaties.    *
* Without the prior written permission of 3Com Corporation and its licensors,*
* any reproduction republication, redistribution, decompiling, reverse      *
* engineering is strictly prohibited. Any unauthorized use of this software  *
* or any portion of it may result in severe civil and criminal penalties, and*
```

```
* will be prosecuted to the maximum extent possible under the applicable law.*
**************************************************************************


Welcome to legal(header legal)
 Press Y or ENTER to continue, N to exit.
Welcome to motd(header motd)
Welcome to login(header login)



Login authentication


Password:
Welcome to shell(header shell)

<Sysname>
```

hotkey

Syntax

hotkey { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_T** | **CTRL_U** } *command*

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

View

System view

Default Level

2: System level

Parameters

CTRL_G: Assigns the hot key **Ctrl+G** to a command.

CTRL_L: Assigns the hot key **Ctrl+L** to a command.

CTRL_O: Assigns the hot key **Ctrl+O** to a command.

CTRL_T: Assigns the hot key **Ctrl+T** to a command.

CTRL_U: Assigns the hot key **Ctrl+U** to a command.

command: The command line associated with the hot key.

Description

Use the **hotkey** command to assign a hot key to a command line.

Use the **undo hotkey** command to restore the default.

By default, the system specifies corresponding commands for **Ctrl+G**, **Ctrl+L** and **Ctrl+O**, while the others are null.

- **Ctrl+G** corresponds to **display current-configuration**

- **Ctrl+L** corresponds to **display ip routing-table**
- **Ctrl+O** corresponds to **undo debugging all**

You can customize this scheme as needed however.

Examples

Assign the hot key **Ctrl+T** to the **display tcp status** command.

```
<Sysname> system-view
[Sysname] hotkey ctrl_t display tcp status
```

Display the configuration of hotkeys.

```
[Sysname] display hotkey
----------------- HOTKEY -----------------

          =Defined hotkeys=
Hotkeys Command
CTRL_G  display current-configuration
CTRL_L  display ip routing-table
CTRL_O  undo debug all
CTRL_T  display tcp status
         =Undefined hotkeys=
Hotkeys Command
CTRL_U  NULL

          =System hotkeys=
Hotkeys Function
CTRL_A  Move the cursor to the beginning of the current line.
CTRL_B  Move the cursor one character left.
CTRL_C  Stop current command function.
CTRL_D  Erase current character.
CTRL_E  Move the cursor to the end of the current line.
CTRL_F  Move the cursor one character right.
CTRL_H  Erase the character left of the cursor.
CTRL_K  Kill outgoing connection.
CTRL_N  Display the next command from the history buffer.
CTRL_P  Display the previous command from the history buffer.
CTRL_R  Redisplay the current line.
CTRL_V  Paste text from the clipboard.
CTRL_W  Delete the word left of the cursor.
CTRL_X  Delete all characters up to the cursor.
CTRL_Y  Delete all characters after the cursor.
CTRL_Z  Return to the user view.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor one word back.
ESC_D   Delete remainder of word.
ESC_F   Move the cursor forward one word.
ESC_N   Move the cursor down a line.
ESC_P   Move the cursor up a line.
ESC_<   Specify the beginning of clipboard.
```

```
ESC_>   Specify the end of clipboard.
```

quit

Syntax

quit

View

Any view

Default Level

0: Visit level (in user view)

2: System level (in other views)

Parameters

None

Description

Use the **quit** command to exit to a lower-level view. If the current view is user view, the **quit** command terminates the current connection and quit the system.

Examples

Switch from GigabitEthernet1/0/1 interface view to system view, and then to user view.

```
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] quit
<Sysname>
```

return

Syntax

return

View

Any view except user view

Default Level

2: System level

Parameters

None

Description

Use the **return** command to return to user view from current view (not user view).

You can also use the hot key **Ctrl+Z** to return to user view from current (not user view).

Related commands: **quit**.

Examples

Return to user view from GigabitEthernet1/0/1 view.

```
[Sysname-GigabitEthernet1/0/1] return
<Sysname>
```

screen-length disable

Syntax

screen-length disable

undo screen-length disable

View

User view

Default Level

1: Monitor level

Parameters

None

Description

Use the **screen-length disable** command to disable the multiple-screen output function of the current user.

Use the **undo screen-length disable** command to enable the multiple-screen output function of the current user.

By default, a login user uses the settings of the **screen-length** command. The default settings of the **screen-length** command are: multiple-screen output is enabled and 24 lines are displayed on the next screen. (For the details of the **screen-length** command, refer to *Login Commands* in the *System Volume*.)

Note that this command is applicable to the current user only and when a user re-logs in, the settings restore to the system default.

Examples

Disable multiple-screen output of the current user.

```
<Sysname> screen-length disable
```

super

Syntax

super [*level*]

View

User view

Default Level

0: Visit level

Parameters

level: User level, in the range 0 to 3, and defaults to 3.

Description

Use the **super** command to switch from the current user privilege level to a specified user privilege level.

If you do not provide the *level* argument, the current user privilege level will be switched to 3.

Login users are classified into four levels that correspond to the four command levels. After users at different levels log in, they can only use commands at their own, or lower, levels.

Note that:

Users can switch to a lower user privilege level unconditionally. However, no password is needed only for AUX login user level switching; to switch to a higher user privilege level, and log in from VTY user interfaces, users need to enter the password needed for the security's sake. If the entered password is incorrect or no password is configured, the switching fails. Therefore, before switching a user to a higher user privilege level, you should configure the password needed.

Related commands: **super password**.

Examples

Set the user privilege level to 2 (The current user privilege level is 3.).

```
<Sysname> super 2
User privilege level is 2, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

Switch the user privilege level back to 3 (Suppose password **123** has been set; otherwise, the user privilege level cannot be switched to 3.).

```
<Sysname> super 3
 Password:
User privilege level is 3, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

super password

Syntax

super password [**level** *user-level*] { **simple** | **cipher** } *password*

undo super password [**level** *user-level*]

View

System view

Default Level

2: System level

Parameters

level *user-level*: User privilege level in the range 1 to 3, with the default as 3.

simple: Plain text password.

cipher: Cipher text password.

password: Password, a string of characters. It is case-sensitive.

- For simple password, it is a string of 1 to 16 characters.
- For cipher password, it is a string of 1 to 16 characters in plain text or 24 characters in cipher text. For example, the simple text “1234567” corresponds to the cipher text “(TT8F]Y\5SQ=^Q`MAF4<1!!”.

Description

Use the **super password** command to set the password needed to switch from a lower user privilege level to a higher one.

Use the **undo super password** command to restore the default.

By default, no password is set to switch from a lower user privilege level to a higher one.

Note that:

- If **simple** is specified, the configuration file saves a simple password.
- If **cipher** is specified, the configuration file saves a cipher password.
- The user must always enter a simple password, no matter **simple** or **cipher** is specified.
- Cipher passwords are recommended, as simple ones are easily getting cracked.

Examples

Set the password to **abc** in simple form for switching user-level to 3.

```
<Sysname> system-view
[Sysname] super password level 3 simple abc
```

Display the password for switching user-level.

```
[Sysname] display current-configuration
#
 super password level 3 simple abc
```

Set the password to abc in cipher form for switching user-level to 3.

```
<Sysname> system-view
[Sysname] super password level 3 cipher abc
```

Display the password for switching user-level.

```
[Sysname] display current-configuration
#
 super password level 3 cipher =`*Y=F>*.%-a_SW8\MYM2A!!
```

sysname

Syntax

sysname sys*name*

undo sysname

View

System view

Default Level

2: System level

Parameters

sysname: Name of the device, a string of 1 to 30 characters.

Description

Use the **sysname** command to set the name of the device.

Use the **undo sysname** demand to restore the device name to the default.

The default name is "**4210G**" by default.

Modifying device name affects the prompt of the CLI. For example, if the device name is **Sysname**, the prompt of user view is <Sysname>.

Examples

Set the name of the device to **Switch**.

```
<Sysname> system-view
[Sysname] sysname Switch
[Switch]
```

system-view

Syntax

system-view

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **system-view** command to enter system view from the current user view.

Related commands: **quit**, **return**.

Examples

Enter system view from the current user view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]
```

4 Device Management Commands

Device Management Commands

boot-loader file

Syntax

boot-loader file *file-url* **slot** { **all** | *slot-number* } { **main** | **backup** }

View

User view

Default Level

2: System level

Parameters

file-url: Specifies a file name, a string of 1 to 63 characters, in the format of [*drive*:/][*path/*]*file-name*, where

- The items in square brackets [ ] are optional.
- *drive* specifies the storage medium of the file. The value is the name of the storage medium. For the switch 4210G, the storage medium can only be a flash.
- *path* specifies the folder of the file. If you do not provide this argument, the file must be in the root directory of the specified storage medium. If the file is saved in a subfolder, you can use this argument multi-times, for example, **test/subtest/test.bin**.
- *file-name* specifies the filename, which is usually suffixed by **.bin**. Suffixes vary with devices.
- If you do not provide arguments *drive* and *path*, the file with the name *file-name* under the current path is specified. You can use the **cd** command to switch to another path. For details of the **cd** command, refer to *File System Management Command*s in the *System Volume*.

slot *slot-number*: Specifies the member ID of a device.

- **all**: Specifies a file as the boot file at the next boot for all member devices in a IRF system.
- *slot-number*: Specifies a file as the boot file at the next boot for a member device. *slot-number* is the member ID of the device. You can use the **display irf** command to view the member IDs of devices in a IRF system.

main: Specifies a file as a main boot file. A main boot file is used to boot a device.

backup: Specifies a file as a backup boot file. A backup boot file is used to boot a device only when a main boot file is unavailable.

Description

Use the **boot-loader** command to specify a boot file for a member device for the next device boot.

Note the following:

- To execute the **boot-loader** command successfully, you must save the file for the next device boot under the root directory of the storage media on a member device.
- If the storage medium is on the master, you can specify the storage medium by giving its name, such as **flash**; if the storage medium is on a slave, you can specify the storage medium by giving its name and the member ID of the device, that is, in the format of slot*slot-number*# *StorageMediumName* (*slot-number* represents the member ID of the salve), such as **slot2#flash**.
- When you specify the boot file of the master, the *file-url* argument cannot contain the member ID of the device, and *slot-number* should be specified as the member ID of the master; when you specify the boot file of the slave, the *file-url* argument must contain the member ID (such as **slot2#flash:/test.bin**), and *slot-number* should be specified as the member ID of the slave.
- If you provide the keyword **all**, the *file-url* argument cannot contain a member ID, otherwise, the execution of this command will fail; you must save the specified boot file on the storage media of all member devices in the same filename, otherwise, member devices without this file will fail to be reconfigured during the reboot.
- The names of the files for the next boot of the master and slaves may be different, but the versions of the files must be the same; otherwise, a slave will reboot by using the master's boot file and join the IRF again.

Related commands: **display boot-loader**.

Examples

Specify the main boot file for the master (the member ID is 1) for the next device boot as **test.bin** (Make sure that the file **test.bin** is already saved on the storage medium of the master; otherwise, the system prompts error and the execution of the commend fails).

```
<Sysname> boot-loader file test.bin slot 1 main
  This command will set the boot file of the specified board. Continue? [Y/N]:y
The specified file will be used as the main boot file at the next reboot on slot 1!
```

Specify the main boot file for the slave (the member ID is 2) for the next device boot as **test.bin** (Make sure that the file **test.bin** is already saved on the storage medium of the slave; otherwise, the system prompts error and the execution of the commend fails).

```
<Sysname> boot-loader file slot2#flash:/test.bin slot 2 main
  This command will set the boot file of the specified board. Continue? [Y/N]:y
The specified file will be used as the main boot file at the next reboot on slot 2!
```

Specify the main boot file for all member devices for the next device boot as **test.bin** (Make sure that the file **test.bin** is already saved on the storage media of all the member devices; otherwise, the system prompts error and the execution of the commend fails).

```
<Sysname> boot-loader file test.bin slot all main
  This command will set the boot file of the specified board. Continue? [Y/N]:y
  The specified file will be used as the main boot file at the next reboot on slot 1!
  The specified file will be used as the main boot file at the next reboot on slot 2!
```

bootrom

Syntax

bootrom update file *file-url* **slot** *slot-number-list*

View

User view

Default Level

2: System level

Parameters

update file *file-url*: Upgrades Boot ROM, *where file-url* is a string of 1 to 63 characters and represents name of the file to be upgraded. *file-url* is in the format of [*drive*:/][*path/*]*file-name*, where

- The items in square brackets [ ] are optional.
- *drive* specifies the storage medium of the file. The value is the name of the storage medium. For the switch 4210G, the storage medium can only be a flash.
- *path* specifies the folder of the file. If you do not provide this argument, the file must be in the root directory of the specified storage medium. If the file is saved in a subfolder, you can use this argument multi-times, for example, **test/subtest/test.bin**.
- *file-name* specifies the filename.
- If you do not provide arguments *drive* and *path*, the file with the name *file-name* under the current path is specified. You can use the **cd** command to switch to another path. For details of the **cd** command, refer to the *File System Management Command*s in the *System Volume*.

slot *slot-number-list*: Specifies a list of IDs of member devices, in the format of { *slot-number* [**to** *slot-number*] }&<1-7>. The *slot-number* argument represents the ID of a member device. You can use the **display irf** command to view the member IDs of IRF members.

Description

Use the **bootrom** command to read, restore, back up, or upgrade the Boot ROM program on a specified member device(s).

Note the following:

- To execute the **bootrom** command successfully, you must save the Boot ROM program under the root directory of the storage media on a member device.
- If the storage medium is on the master, you can specify the storage medium by giving its name, such as **flash**; If a storage medium is on a slave, you can specify the storage medium by giving its name and the member ID of the device, that is, in the format of slot*slot-number*# *StorageMediumName* (*slot-number* represents the member ID of the slave), such as **slot2#flash**.
- When you upgrade the Boot ROM program for the master, the *file-url* argument cannot contain the member ID of the device, and *slot-number* should be specified as the member ID of the master; when you upgrade the Boot ROM program for a slave, the *file-url* argument must contain the member ID (such as **slot2#flash:/test.bin**), *slot-number* should be specified as the member ID of the slave.

Examples

Use the **a.btm** file to upgrade the Boot ROM program on the master (the member ID is 1).

```
<Sysname> bootrom update file a.btm slot 1
  This command will update bootrom file on the specified board(s), Continue? [Y/N]:y
  This command will update bootrom file on the specified board(s), Continue? [Y/N]:y
  Now updating bootrom, please wait...
  Succeeded to update bootrom of Board 1.
```

Use the **a.btm** file to upgrade the Boot ROM program on the slave (the member ID is 2).

```
<Sysname> bootrom update file slot2#flash:/a.btm slot 2
  This command will update bootrom file on the specified board(s), Continue? [Y/N]:y
  Now updating bootrom, please wait...
  Succeeded to update bootrom of Board 1
```

bootrom-update security-check enable

Syntax

bootrom-update security-check enable

undo bootrom-update security-check enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **bootrom-update security-check enable** command to enable the validity check function.

Use the **undo bootrom-update security-check enable** command to disable the validity check function.

By default, the validity check function is enabled at the time of upgrading Boot ROM.

After the validity check function is enabled, the device will strictly check whether the Boot ROM upgrade files are valid and can match the hardware.

Examples

Enable the validity check function when upgrading Boot ROM.

```
<Sysname> system-view
[Sysname] bootrom-update security-check enable
```

display boot-loader

Syntax

display boot-loader [**slot** *slot-number*]

View

Any view

Default Level

2: System level

Parameters

slot *slot-number*: Displays boot file information of a member device, where *slot-number* represents the member ID of the device. If you do not provide this argument, the information of the boot files of all member devices will be displayed. You can use the **display irf** command to view the member IDs of devices in a IRF system.

Description

Use the **display boot-loader** command to display information of the boot file.

Related commands: **boot-loader.**

Examples

Display the file adopted for the current and next boot of the device.

```
<Sysname> display boot-loader
 Slot 12
The current boot app is:  flash:/test.bin
The main boot app is:    flash:/test.bin
The backup boot app is:   flash:/test.bin
```

Table 4-1 display boot-loader command output description

Field	Description
Slot 1	The member ID of the device is 1
The current boot app is	Boot file used for the device for the current device boot
The main boot app is	Main boot file used for the device for the next device boot
The backup boot app is	Backup boot file used for the device for the next device boot

display cpu-usage

Syntax

display cpu-usage [**slot** *slot-number* [**cpu** *cpu-number*]]

display cpu-usage *entry-number* [*offset*] [**verbose**] [**slot** *slot-number* [**cpu** *cpu-number*]] [**from-device**]

View

Any view

Default Level

1: Monitor level

Parameters

entry-number: Number of entries to be displayed once, in the range 1 to 60.

offset: Offset between the serial number of the first CPU usage statistics record to be displayed and that of the last CPU usage record to be displayed, in the range 0 to 59. For example, the idx of the latest statistics record is 12, if the *offset* is set to 3, the system will display the statistics records from

the one with the idx of 9. idx represents the serial number of the period for the statistics, and its value ranges from 0 to 60 cyclically. The system makes CPU usage statistics periodically; after each period, the system records the average CPU usage during this period, and the idx value is added by 1 automatically.

verbose: Specifies to display detailed information of CPU usage statistics. If this keyword is not provided, the system displays the brief information of the CPU usage statistics; if this keyword is provided, the system displays the average CPU usage statistics for each task in the specified period.

from-device: Displays external storage media. The device currently does not support the **from-device** keyword.

slot *slot-number*: Indicates to display the statistics of the CPU usage of the specified member device. *slot-number* specifies the member ID of the device. You can use the **display irf** command to view the member IDs of devices in a IRF system.

cpu *cpu-number*: Displays the CPU usage statistics of the specified CPU. If the *cpu-number* argument is not provided, the system displays the CPU usage statistics of all CPUs of the specified board or member device.

Description

Use the **display cpu-usage** command to display the CPU usage statistics.

The system takes statistics of CPU usage at intervals (usually every 60 seconds) and saves the statistical results in the history record area. **display cpu-usage** *entry-number* indicates the system displays *entry-number* records from the newest (last) record. **display cpu-usage** *entry-number offset* indicates the system displays *entry-number* records from the last but *offset* record.

Equivalent to the **display cpu-usage 1 0 verbose** command, the **display cpu-usage** command displays detailed information of the last CPU usage statistics record.

Examples

Display information of the current CPU usage statistics.

```
<Sysname> display cpu-usage
Slot 1 CPU usage:
      6% in last 5 seconds
     10% in last 1 minute
      5% in last 5 minutes
Slot 2 CPU usage:
      5% in last 5 seconds
      8% in last 1 minute
      5% in last 5 minutes
```

Display the last fifth and sixth records of the CPU usage statistics history.

```
<Sysname> display cpu-usage 2 4
===== CPU usage info (no:  0  idx: 58) =====
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage          : 3%
CPU Usage Stat. Time : 2006-07-10  10:56:55
CPU Usage Stat. Tick : 0x1d9d(CPU Tick High) 0x3a659a70(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x95030517(CPU Tick Low)

===== CPU usage info (no:  1  idx: 57) =====
```

```
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage          : 3%
CPU Usage Stat. Time : 2006-07-10  10:55:55
CPU Usage Stat. Tick : 0x1d9c(CPU Tick High) 0xa50e5351(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x950906af(CPU Tick Low)
```

Table 4-2 display cpu-usage command output description

Field	Description
6% in last 5 seconds	After the device boots, the system calculates and records the average CPU usage in every five seconds. This field displays the average CPU usage in the last five seconds.
10% in last 1 minute	After the device boots, the system calculates and records the average CPU usage in every one minute. This field displays the average CPU usage in the last minute.
5% in last 5 minutes	After the device boots, the system calculates and records the average CPU usage in every five minutes. This field displays the average CPU usage in the last five minutes.
Slot 2 CPU usage	The CPU usage of the member device (the member ID is 2).
CPU usage info (no: idx:)	Information of CPU usage records (no: The (no+1)th record is currently displayed. no numbers from 0, a smaller number equals a newer record. idx: index of the current record in the history record table). If only the information of the current record is displayed, no and idx are not displayed.
CPU Usage Stat. Cycle	CPU usage measurement interval, in seconds. For example, if the value is 41, it indicates that the average CPU usage during the last 41 seconds is calculated. The value range of this field is 1 to 60.
CPU Usage	Average CPU usage in a measurement interval, in percentage
CPU Usage Stat. Time	CPU usage statistics time in seconds, that is, the system time when the command is executed
CPU Usage Stat. Tick	System runtime in ticks, represented by a 64-bit hexadecimal. CPU Tick High represents the most significant 32 bits and the CPU Tick Low the least significant 32 bits.
Actual Stat. Cycle	Actual CPU usage measurement interval in ticks, represented by a 64-bit hexadecimal. CPU Tick High represents the most significant 32 bits and the CPU Tick Low the least significant 32 bits. Owing to the precision of less than one second, the actual measurement periods of different CPU usage records may differ slightly.

display cpu-usage history

Syntax

display cpu-usage history [**task** *task-id*] [**slot** *slot-number* [**cpu** *cpu-number*]]

View

Any view

Default Level

1: Monitor level

Parameters

task *task-id*: Displays the history statistics of the CPU usage of the specified task, where *task-id* represents the task number. If the *task-id* argument is not provided, the system displays the history statistics of the CPU usage of the entire system (the CPU usage of the entire system is the sum of CPU usages of all tasks).

slot *slot-number*: Displays the history statistics of the CPU usage of the specified member device. *slot-number* specifies the member ID of a device. You can use the **display irf** command to view the member IDs of devices in a IRF system. If the *slot-number* argument is not provided, the system displays the history statistics of the CPU usage of the master.

cpu *cpu-number*: Displays the history statistics of the CPU usage of the specified CPU. If the *cpu-number* argument is not provided, the system displays the history statistics of the CPU usage of the main CPU.

Description

Use the **display cpu-usage history** command to display the history statistics of the CPU usage in a chart.

If no argument is provided, the system displays the CPU usage of the master.

The system takes statistics of the CPU usage at an interval and saves the statistical results in the history record area. You can use the **display cpu-usage history** command to display the CPU usage statistics records during the last 60 minutes. The statistical results are displayed through geographical coordinates. In the output information:

- Latitude indicates the CPU usage, which is displayed based on the step. For example, if the step of the CPU usage is 5%, then the actual statistics value 53% is displayed as 55%, and actual statistics value 52% is displayed as 50%.
- Longitude indicates the time.
- Consecutive pond marks (#) indicate the CPU usage at a certain moment. The value of the latitude corresponding to the # mark on the top of a moment is the CPU usage at this moment.

Examples

Display the CPU usage statistics of the whole system.

```
<Sysname> display cpu-usage history
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
```

```
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|           #
 10%|          ###  #
  5%|         ########
    ------------------------------------------------------------
            10       20       30       40       50       60  (minutes)
                   cpu-usage last 60 minutes(SYSTEM)
```

The above output information indicates the CPU usage of the whole system in the last 60 minutes: 5% in the twelfth minute, 10% in the thirteenth minute, 15% in the fourteenth minute, 10% in the fifteenth minute, 5% in the sixteenth and seventeenth minute, 10% in the eighteenth minute, 5% in the nineteenth minute, and 2% or lower than 2% at other times.

Display the CPU usage statistics of task 6.

```
<Sysname> display cpu-usage history task 6
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|
 10%|
  5%|                #
    ------------------------------------------------------------
            10       20       30       40       50       60  (minutes)
                   cpu-usage last 60 minutes(T03M)
```

The above output information indicates the CPU usage of task 6 (with the task name **T03M**) in the last 60 minutes: 5% in the twentieth minute, and 2% or lower than 2% at other times.

display device

Syntax

display device [[**shelf** *shelf-number*] [**frame** *frame-number*] [**slot** *slot-number* [**subslot** *subslot-number*]] | **verbose**]

View

Any view

Default Level

2: System level

Parameters

shelf *shelf-number*: Displays detailed information of the specified shelf or unit. The *shelf-number* argument represents a shelf number or unit number and the value is 0 for the switch 4210G.

frame *frame-number*: Displays detailed information of the specified frame. The *frame-number* argument represents a frame number and the value is 0 for the switch 4210G.

slot *slot-number*: Displays information of the specified member device. The *slot-number* argument represents the member ID of the device. You can use the **display irf** command to view the member IDs of devices in a IRF system.

subslot *subslot-number*: Displays information of the specified subboard. The *subslot-number* represents the subslot of a subboard.

verbose: Displays detailed information.

Description

Use the **display device** command to display information about the device.

Examples

Display the information of all IRF members.

```
<Sysname> display device
 Slot 1
SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type      State
0      28      REV.C  NULL    002     505       IVL    MAIN      Normal
1      0       REV.A  NULL    NULL    NULL      IVL    2*10GE    Normal
 Slot 2
SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type      State
0      28      REV.C  NULL    002     503       IVL    MAIN      Normal
1      0       REV.B  NULL    NULL    NULL      IVL    2*10GE    Normal
```

The above information indicates that the IRF contains two member devices, each of which has 28 Ethernet interfaces and is configured with two 10 GE physical IRF ports.

Table 4-3 display device command output description

Field	Description
Slot 1	Information of the device with the member ID of 1
SubSNo	Number of the slot in which the subboard resides

Field	Description
PortNum	Maximum number of ports that a subboard supports
AddrLM	Address learning mode

display device manuinfo

Syntax

display device manuinfo

View

Any view

Default Level

3: Manage level

Parameters

None

Description

Use the **display device manuinfo** command to display electrical label information about the device.

Electrical label information is also called permanent configuration data or archive information, which is written to the storage medium of the device during debugging or test of device. The information includes name of the board, device serial number, and vendor name. This command displays part of the electrical label information of the device.

Examples

Display electrical label information.

```
<Sysname> display device manuinfo
slot 1
DEVICE_NAME         : S4210G-28C-EI
DEVICE_SERIAL_NUMBER : 210235A2540000000001
MAC_ADDRESS         : 001C-C5BC-3111
MANUFACTURING_DATE   : 2008-05-08
VENDOR_NAME         : 3COM
slot 2
DEVICE_NAME         : S4210G-28C-EI
DEVICE_SERIAL_NUMBER : 210235A252A079000140
MAC_ADDRESS         : 000F-E269-46D1
MANUFACTURING_DATE   : 2007-09-26
VENDOR_NAME         : 3COM
```

Table 4-4 display device manuinfo command output description

Field	Description
DEVICE_NAME	Device name

Field	Description
DEVICE_SERIAL_NUMBER	Device serial number
MAC_ADDRESS	MAC address of the device
MANUFACTURING_DATE	Manufacturing date of the device
VENDOR_NAME	Vendor name

display environment

Syntax

display environment

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display environment** command to display the temperature information, including the current temperature and temperature thresholds of boards.

Examples

Display the temperature information of the device.

```
<Sysname> display environment
System Temperature information (degree centigrade):
-------------------------------------------------
 SlotNo    Temperature      Lower limit     Upper limit
 1         34               0               55
 2         34               0               55
```

Table 4-5 display environment command output description

Field	Description
System Temperature information (degree centigrade)	Temperature information of system boards (degree centigrade)
SlotNO	Member ID of the device
Temperature	Current temperature
Lower limit	Lower limit of temperature
Upper limit	Upper limit of temperature

display fan

Syntax

display fan [**slot** *slot-number* [*fan-id*]]

View

Any view

Default Level

1: Monitor level

Parameters

fan-id: Displays the operating state of the specified fan, where *fan-id* represents the built-in fan number.

slot *slot-number*: Displays the operating state of fans of the specified member device, where *slot-number* represents the member ID of the device. Support for **slot** *slot-number* depends on the device model. You can use the **display irf** command to view the member IDs of devices in a IRF system. If the *slot-number* argument is not provided, the system displays the operating state of fans of all member devices.

Description

Use the **display fan** command to display the operating state of built-in fans.

Examples

Display the operating state of all fans in a device.

```
<Sysname> display fan
 Slot 1
     FAN    1
     State    : Normal
 Slot 2
     FAN    1
     State    : Normal
```

display memory

Syntax

display memory [**slot** *slot-number* [**cpu** *cpu-number*]]

View

Any view

Default Level

1: Monitor level

Parameters

slot *slot-number*: Displays the memory of a CPU of the specified member device, where *slot-number* represents the member ID of the device. You can use the **display irf** command to view the member IDs of devices in a IRF system.

cpu *cpu-number:* Displays the memory of a specified CPU, where *cpu-number* represents the ID of the CPU.

Description

Use the **display memory** command to display the usage of the memory of a device.

If the keyword **slot** is not provided, the system displays the usage of the memory of the master device; if the keyword **cpu** is not provided, the system displays the memory of the main CPU.

Examples

Display the usage of the memory of a device.

```
<Sysname> display memory
System Total Memory(bytes): 431869088
Total Used Memory(bytes): 71963156
Used Rate: 16%
```

Table 4-6 display memory command output description

Field	Description
System Total Memory(bytes)	Total size of the system memory (in bytes)
Total Used Memory(bytes)	Size of the memory used (in bytes)
Used Rate	Percentage of the memory used to the total memory

display power

Syntax

display power [**slot** *slot-number* [*power-id*]]

View

Any view

Default Level

1: Monitor level

Parameters

slot *slot-number*: Displays the status of the power supply of the specified device in an IRF, where *slot-number* represents the member ID of the device. You can use the **display irf** command to view the member IDs of devices in a IRF system.

power-id: Displays the status of the specified power supply unit (PSU), where *power-id* represents the PSU number. The value varies with devices.

Description

Use the **display power** command to display the status of the power supply of a device.

Examples

Display the status of the power supply of a device.

```
<Sysname> display power
Slot 1
     Power    1
     State    : Normal
     Type     : AC

 Slot 2
     Power    1
     State    : Normal
     Type     : AC
```

display reboot-type

Syntax

display reboot-type [**slot** *slot-number*]

View

Any view

Default Level

2: System level

Parameters

slot *slot-number*: Displays reboot mode of the specified member device, where *slot-number* represents the member ID of the device. You can use the **display irf** command to view the member IDs of devices in a IRF system.

Description

Use the **display reboot-type** command to display the reboot mode of the device.

If no keyword is provided, the system displays the reboot mode of the master.

Examples

Display the reboot mode of the device.

```
<Sysname> display reboot-type
  The rebooting type this time is: Cold
```

The above information indicates that the last reboot mode of the device is Cold boot (cold boot is to restart a device by powering it on). (The display of Warm represents a warm boot, which means to restart a device by using the commands like **reboot**).

display rps

Syntax

display rps [**slot** *slot-number* [*rps-id*]]

View

Any view

Default Level

1: Monitor level

Parameters

slot *slot-number*: Displays the RPS status of the specified member device, where *slot-number* represents the member ID of the device. You can use the **display irf** command to view the member IDs of devices in a IRF system. If the *slot-number* argument is not provided, the system displays the RPS status of all IRF members.

rps-id: Displays the status of the specified RPS, where *rps-id* represents the RPS number. The value varies with devices.

Description

Use the **display rps** command to display status of the RPS.

Examples

Display RPS status of the device.

```
<Sysname> display rps
Slot 1
     Power    2
     State    : Absent

 Slot 2
     Power    2
     State    : Absent
```

display schedule job

Syntax

display schedule job

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display schedule job** command to display the detailed configurations of the scheduled automatic execution function.

Examples

Display the detailed configurations of the current scheduled automatic execution function.

```
<Sysname> display schedule job
Specified command: execute 1.bat
Specified view: system view
Executed time: at 12:00 10/31/2007 (in 0 hours and 16 minutes)
```

If you modify the system time within 16 minutes, the configurations of scheduled automatic execution of the batch file will become invalid, and then when you execute the **display schedule job** command again, the system displays nothing.

display schedule reboot

Syntax

display schedule reboot

View

Any view

Default Level

3: Manage level

Parameters

None

Description

Use the **display schedule reboot** command to display the device reboot time set by the user.

Related commands: **schedule reboot at** and **schedule reboot delay.**

Examples

Display the reboot time of a device.

```
<Sysname> display schedule reboot
System will reboot at 16:00:00 03/10/2006 (in 2 hours and 5 minutes).
```

The above information indicates the system will reboot at 16:00:00 on March 10, 2006 (in two hours and five minutes).

display system-failure

Syntax

display system-failure

View

Any view

Default Level

3: Manage level

Parameters

None

Description

Use the **display system-failure** command to display the exception handling method of all member devices in a IRF system.

Related commands: **system-failure**.

Examples

Display the exception handling method.

```
<Sysname> display system-failure
 System failure handling method: reboot
```

display transceiver alarm

Syntax

display transceiver alarm interface *interface-type interface-number*

View

Any view

Default Level

2: System level

Parameters

interface [*interface-type interface-number*]: Displays the current alarm information of the pluggable transceiver plugged in the specified interface. *interface-type interface-number* represents interface type and interface number. If it is not specified, the command displays the current alarm information of the pluggable transceiver in all the interfaces.

Description

Use the **display transceiver alarm** command to display the current alarm information of a single or all transceivers.

If no error occurs, **None** is displayed.

Table 4-7 shows the alarm information that may occur for the four types of commonly used transceivers.

Table 4-7 display transceiver alarm command output description

Field	Remarks
GBIC/SFP	
RX loss of signal	Incoming (RX) signal is lost.
RX power high	Incoming (RX) power level is high.

Field	Remarks
RX power low	Incoming (RX) power level is low.
TX fault	Transmit (TX) fault
TX bias high	TX bias current is high.
TX bias low	TX bias current is low.
TX power high	TX power is high.
TX power low	TX power is low.
Temp high	Temperature is high.
Temp low	Temperature is low.
Voltage high	Voltage is high.
Voltage low	Voltage is low.
Transceiver info I/O error	Transceiver information read and write error
Transceiver info checksum error	Transceiver information checksum error
Transceiver type and port configuration mismatch	Transceiver type does not match port configuration.
Transceiver type not supported by port hardware	Transceiver type is not supported on the port.
XFP	
RX loss of signal	Incoming (RX) signal is lost.
RX not ready	RX is not ready
RX CDR loss of lock	RX clock cannot be recovered.
RX power high	RX power is high.
RX power low	RX power is low.
TX not ready	TX is not ready.
TX fault	TX fault
TX CDR loss of lock	TX clock cannot be recovered.
TX bias high	TX bias current is high.
TX bias low	TX bias current is low.
TX power high	TX power is high.
TX power low	TX power is low.
Module not ready	Module is not ready.
APD supply fault	APD (Avalanche Photo Diode) supply fault
TEC fault	TEC (Thermoelectric Cooler) fault
Wavelength unlocked	Wavelength of optical signal exceeds the manufacturer’s tolerance.
Temp high	Temperature is high.
Temp low	Temperature is low.
Voltage high	Voltage is high.

Field	Remarks
Voltage low	Voltage is low.
Transceiver info I/O error	Transceiver information read and write error
Transceiver info checksum error	Transceiver information checksum error
Transceiver type and port configuration mismatch	Transceiver type does not match port configuration.
Transceiver type not supported by port hardware	Transceiver type is not supported on the port.
XENPAK	
WIS local fault	WIS (WAN Interface Sublayer) local fault
Receive optical power fault	Receive optical power fault
PMA/PMD receiver local fault	PMA/PMD (Physical Medium Attachment/Physical Medium Dependent) receiver local fault
PCS receive local fault	PCS (Physical Coding Sublayer) receiver local fault
PHY XS receive local fault	PHY XS (PHY Extended Sublayer) receive local fault
RX power high	RX power is high.
RX power low	RX power is low.
Laser bias current fault	Laser bias current fault
Laser temperature fault	Laser temperature fault
Laser output power fault	Laser output power fault
TX fault	TX fault
PMA/PMD receiver local fault	PMA/PMD receiver local fault
PCS receive local fault	PCS receive local fault
PHY XS receive local fault	PHY XS receive local fault
TX bias high	TX bias current is high.
TX bias low	TX bias current is low.
TX power high	TX power is high.
TX power low	TX power is low.
Temp high	Temperature is high.
Temp low	Temperature is low.
Transceiver info I/O error	Transceiver information read and write error
Transceiver info checksum error	Transceiver information checksum error
Transceiver type and port configuration mismatch	Transceiver type does not match port configuration.
Transceiver type not supported by port hardware	Transceiver type is not supported on the port.

Examples

Display the alarm information of the pluggable transceiver plugged in interface GigabitEthernet1/0/1. (The output of this command varies with devices.)

```
<Sysname> display transceiver alarm interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 transceiver current alarm information:
  RX loss of signal
  RX power low
```

Table 4-8 display transceiver alarm command output description

Field	Description
transceiver current alarm information	Current alarm information of the transceiver
RX loss of signal	Incoming (RX) signal is lost.
RX power low	Incoming (RX) power level is low.

display transceiver diagnosis

Syntax

display transceiver diagnosis interface [*interface-type interface-number*]

View

Any view

Default Level

2: System level

Parameters

interface [*interface-type interface-number*]: Displays the currently measured value of digital diagnosis parameters of the 3COM customized anti-spoofing pluggable optical transceiver plugged in the specified interface. *interface-type interface-number* represents interface type and interface number. If it is not specified, the command displays the currently measured value of digital diagnosis parameters of 3COM customized anti-spoofing pluggable optical transceivers in all the interfaces.

Description

Use the **display transceiver diagnosis** command to display the currently measured value of digital diagnosis parameters of 3COM customized anti-spoofing pluggable optical transceivers.

Examples

Display the currently measured value of the digital diagnosis parameters of the 3COM customized anti-spoofing pluggable optical transceiver plugged in interface GigabitEthernet1/0/2.

```
<Sysname> display transceiver diagnosis interface gigabitethernet1/0/2
GigabitEthernet1/0/2 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp(°C)  Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    36        3.31        6.13      -35.64         -5.19
```

Table 4-9 display transceiver diagnosis command output description

Field	Description
transceiver diagnostic information	Digital diagnosis information of the transceiver plugged in the interface
Current diagnostic parameters	Current diagnostic parameters
Temp.(°C)	Digital diagnosis parameter-temperature, in °C, with the precision to 1°C.
Voltage(V)	Digital diagnosis parameter-voltage, in V, with the precision to 0.01 V.
Bias(mA)	Digital diagnosis parameter-bias current, in mA, with the precision to 0.01 mA.
RX power(dBM)	Digital diagnosis parameter-RX power, in dBM, with the precision to 0.01 dBM.
TX power(dBM)	Digital diagnosis parameter-TX power, in dBM, with the precision to 0.01 dBM.

display transceiver

Syntax

display transceiver interface [*interface-type interface-number*]

View

Any view

Default Level

2: System level

Parameters

interface [*interface-type interface-number*]: Displays main parameters of the pluggable transceiver plugged in the specified interface. *interface-type interface-number* represents interface type and interface number. If it is not specified, the command displays main parameters of the pluggable transceiver(s) in all the interfaces.

Description

Use the **display transceiver** command to display main parameters of a single or all pluggable transceivers.

Examples

Display main parameters of the pluggable transceiver plugged in interface GigabitEthernet1/0/3.

```
<Sysname> display transceiver interface gigabitethernet1/0/3
GigabitEthernet1/0/3 transceiver information:
  Transceiver Type            : 1000_BASE_SX_SFP
  Connector Type              : LC
  Wavelength(nm)              : 850
  Transfer Distance(m)         : 550(50um),270(62.5um)
```

```
Digital Diagnostic Monitoring : YES
Vendor Name                   : 3COM
Ordering Name                 : SFP-GE-SX-MM850
```

Table 4-10 display transceiver command output description

Field	Description
transceiver information	Pluggable transceiver information
Transceiver Type	Pluggable transceiver type
Connector Type	Type of the connectors of the transceiver: • Optical connectors, including SC (SC connector, developed by NTT) and LC (LC connector, 1.25 mm/RJ-45 optical connector developed by Lucent). • Other connectors, including RJ-45 and CX 4.
Wavelength(nm)	• Optical transceiver: central wavelength of the laser sent, in nm. If the transceiver supports multiple wavelengths, every two wavelength values are separated by a comma. • Electrical transceiver: displayed as N/A.
Transfer distance(xx)	Transfer distance, with xx representing km for single-mode transceivers and m for other transceivers. If the transceiver supports multiple transfer medium, every two values of the transfer distance are separated by a comma. The corresponding transfer medium is included in the bracket following the transfer distance value. The following are the transfer media: • 9 um: 9/125 um single-mode fiber • 50 um: 50/125 um multi-mode fiber • 62.5 um: 62.5/125 um multi-mode fiber • TP: Twisted pair • CX4: CX4 cable
Digital Diagnostic Monitoring	Whether the digital diagnosis function is supported, where: • YES: supported • NO: not supported
Vendor Name	Vendor name or name of the vendor who customizes the transceiver: • 3COM customized anti-spoofing transceiver: **3COM** is displayed. • Other transceivers: The vendor name is displayed.
Ordering Name	Pluggable transceiver model

display transceiver manuinfo

Syntax

display transceiver manuinfo interface [*interface-type interface-number*]

View

Any view

Default Level

2: System level

Parameters

interface [*interface-type interface-number*]: Displays part of the electrical label information of the 3COM customized anti-spoofing pluggable transceiver plugged in the specified interface. *interface-type interface-number* represents interface type and interface number. If it is not specified, the command displays part of the electrical label information of the 3COM customized anti-spoofing pluggable transceiver(s) in all the interfaces.

Description

Use the **display transceiver manuinfo** command to display part of the electrical label information of a single or all 3COM customized anti-spoofing pluggable transceivers.

Examples

Display the electrical label information of the 3COM customized anti-spoofing pluggable transceiver plugged in interface GigabitEthernet1/0/4.

```
<Sysname> display transceiver manuinfo interface gigabitethernet1/0/4
GigabitEthernet1/0/4 transceiver manufacture information:
  Manu. Serial Number  : 213410A0000054000251
  Manufacturing Date   : 2006-09-01
  Vendor Name          : 3COM
```

Table 4-11 display transceiver manuinfo command output description

Field	Description
Manu. Serial Number	Serial number generated during debugging and testing of the customized transceivers
Manufacturing Date	Debugging and testing date. The date takes the value of the system clock of the computer that performs debugging and testing.
Vendor Name	Name of the vendor who customizes the transceiver, that is, 3COM.

reboot

Syntax

reboot [**slot** *slot-number*]

View

User view

Default Level

2: System level

Parameters

slot *slot-number*: Specifies the slot number of a member device. You can use the **display irf** command to view the member IDs of devices in a IRF system.

Description

Use the **reboot** command to reboot a member device, a subboard, or the whole IRF system.

You can use the **reboot** [**slot** *slot-number*] command on the master to reboot the master or a slave.

If the **slot** keyword is not provided, the whole IRF system will reboot.

Caution

- Device reboot may result in the interruption of the ongoing services. Use these commands with caution.
- If a main boot file fails or does not exist, the device cannot be rebooted with the **reboot** command. In this case, you can re-specify a main boot file to reboot the device, or you can power off the device, then power it on and the system automatically uses the backup boot file to restart the device.
- If you are performing file operations when the device is to be rebooted, the system does not execute the command for the sake of security.

Examples

If the current configuration does not change, reboot the device.

```
<Sysname> reboot
 Start to check configuration with next startup configuration file, please wait.........DONE!
 This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

If the current configuration changes, reboot the device.

```
<Sysname> reboot
 Start to check configuration with next startup configuration file, please wait.........DONE!
 This command will reboot the device. Current configuration will be lost in next startup if
you continue. Continue? [Y/N]:y
Now rebooting, please wait...
```

reset unused porttag

Syntax

reset unused porttag

View

User view

Default Level

1: Monitor level

Parameters

None

Description

Use the **reset unused porttag** command to clear the 16-bit index saved but not used in the current systems of all member devices.

A confirmation is required when you carry out this command. If you fail to make a confirmation within 30 seconds or enter “N” to cancel the operation, the command will not be carried out.

Examples

Clear the 16-bit index saved but not used in the current system.

```
<Sysname> reset unused porttag
Current operation will delete all unused port tag(s). Continue? [Y/N]:y
<Sysname>
```

schedule job

Syntax

schedule job { **at** *time1* [*date*] | **delay** *time2* } **view** *view command*

undo schedule job

View

User view

Default Level

3: Manage level

Parameters

at *time1* [*date*]: Specifies the execution time of a specified command.

- *time1*: Execution time of the command, in the format of *hh:mm* (hour/minute). The *hh* value ranges from 0 to 23, and the *mm* value ranges from 0 to 59. The value of *hh:mm* cannot exceed 23:59.
- *date*: Execution date of the command, in the format of *MM/DD/YYYY* (month/day/year) or *YYYY/MM/DD* (year/month/day). The *YYYY* value ranges from 2000 to 2035, the *MM* value ranges from 1 to 12, and the *DD* value range depends on a specific month.

delay *time2*: Specifies the execution waiting time of a specified command. *time2 represents the waiting time,* which can be in the following format:

- *hh:mm* (hour/minute): The *hh* value ranges from 0 to 720, and the *mm* value ranges from 0 to 59. The value of *hh:mm* cannot exceed 720:00.
- *mm* (minute): It ranges from 0 to 432000, with 0 indicating that a command is executed immediately without any delay.

view *view*: Specifies the view in which a command is executed. *view* represents the view name, and it takes the following values at present:

- **shell**, represents user view.
- **system**, represents system view.

command: The command string to be automatically executed at the scheduled time.

Description

Use the **schedule job** command to automatically execute a specified command at the scheduled time.

Use the **undo schedule job** command to remove the configuration.

Note the following:

- If you provide both the *time1* and *date* arguments, the execution time must be a future time.
- If you only provide the *time1* argument, when *time1* is earlier than the current system time, the specified command is executed at *time1* of the next day; when *time1* is later than the current system time, the specified command is executed at *time1* of the current day.
- No matter whether you use the **at** or **delay** keyword, the difference between the execution time of a command and the current system time cannot exceed 720 hours (namely, 30 days).
- At present, you can specify only user view and system view. To automatically execute the specified commands in other views or automatically execute multiple commands at a time, you can configure the system to automatically execute a batch file at a specified time (note that you must provide a complete file path for the system to execute the batch file.).
- The system does not check the *view* and *command* arguments. Therefore, ensure the correctness of the *command* argument (including the correct format of *command* and the correct relationship between the *command* and *view* arguments.).
- After the specified automatic execution time is reached, the system executes the specified commands without displaying any information except system information such as log, trap and debug.
- When the system is executing the specified command, you do not need to input any information. If there is information for you to confirm, the system automatically inputs **Y** or **Yes**; if certain characters need to be input, the system automatically inputs a default character string, and inputs an empty character string when there is no default character string.
- For the commands used to switch user interfaces, such as **telnet**, **ftp**, and **ssh2**, the commands used to switch views, such as **system-view**, **quit** and **interface ethernet**, and the commands used to modify status of the user that is executing commands, such as **super**, the operation interface, command view and status of the current user are not changed after the automatic execution function is performed.
- If you modify the system time after the automatic execution function is configured, the scheduled automatic execution configuration turns invalid automatically.
- Only the latest configuration takes effect if you execute the **schedule job** command repeatedly.

Examples

Configure that the device will execute the batch file **1.bat** in system view in 60 minutes (supposing that the current time is 11:43).

```
<Sysname> schedule job delay 60 view system execute 1.bat
Info: Command execute 1.bat in system view will be executed at 12:43 10/31/2007 (in 1 hours
and 0 minutes).
```

Configure that the device will execute the batch file **1.bat** in system view at 12:00 in the current day (supposing that the current time is 11:43).

```
<Sysname> schedule job at 12:00 view system execute 1.bat
Info: Command execute 1.bat in system view will be executed at 12:00 10/31/2007 (in 0 hours
and 16 minutes).
```

schedule reboot at

Syntax

schedule reboot at *hh:mm* [*date*]

undo schedule reboot

View

User view

Default Level

3: Manage level

Parameters

hh:mm: Reboot time of a device, in the format of hh:mm (hours:minutes). The value of the *hh* argument ranges from 0 to 23, and the value of the *mm* argument ranges from 0 to 59.

date: Reboot date of a device, in the format mm/dd/yyyy (month/day/year) or in the format yyyy/mm/dd (year/month/day) The yyyy value ranges from 2000 to 2035, the mm value ranges from 1 to 12, and the dd value depends on a specific month.

Description

Use the **schedule reboot at** command to enable the scheduled reboot function on all member devices and specify a specific reboot time and date.

Use the **undo schedule reboot** command to disable the scheduled reboot function.

By default, the scheduled reboot function is disabled.

There are two cases if no specific reboot date is specified:

- When the specified reboot time is later than the current time, the device will be rebooted at the reboot time of the current day.
- When the specified reboot time is earlier than the current time, the device will be rebooted at the reboot time the next day.
- If you are performing file operations when the device is to be rebooted, the system does not execute the command for the sake of security.

Note that:

- The precision of the device timer is 1 minute. One minute before the reboot time, the device will prompt “REBOOT IN ONE MINUTE” and will be rebooted in one minute.
- The difference between the reboot date and the current date cannot exceed 30 x 24 hours (namely, 30 days).
- After you execute the above command, the device will prompt you to confirm the configuration. You must enter **Y** or **y** to make the configuration take effect. The original configuration will be overwritten at the same time.
- If a date (month/day/year or year/month/day) later than the current date is specified for the **schedule reboot at** command, the device will be rebooted at the reboot time.
- If you use the **clock** command after the **schedule reboot at** command to adjust the system time, the reboot time set by the **schedule reboot at** command will become invalid.

 **Caution**

This command reboots the device in a future time, thus resulting in service interruption. Please use it with caution.

Examples

Configure the device to reboot at 12:00 AM (supposing that the current time is 11:43).

```
<Sysname> schedule reboot at 12:00
Reboot system at 12:00 06/06/2006(in 0 hour(s) and 16 minute(s))
 confirm? [Y/N]:
```

If you have used the **terminal logging** command to enable the log display function on the terminal before setting a reboot time, the system will automatically display related log information after you enter <y>. By default, the log display function is enabled.

```
<Sysname>
%Jun  6 11:43:11:629 2006 Sysname CMD/4/REBOOT:
vty0(192.168.1.54): Set schedule reboot parameters at 11:43:11 06/06/2006, and system will
reboot at 12:00 06/06/2006.
```

schedule reboot delay

Syntax

schedule reboot delay { *hh:mm* | *mm* }

undo schedule reboot

View

User view

Default Level

3: Manage level

Parameters

hh:mm: Device reboot wait time, in the format of hh:mm (hours:minutes). The value of the *hh* argument ranges from 0 to 720, and the value of the *mm* argument ranges from 0 to 59, and the value of the *hh:mm* argument cannot exceed 720:00.

mm: Device reboot wait time in minutes, in the range of 0 to 43,200.

Description

Use the **schedule reboot delay** command to enable the scheduled reboot function of all member devices and set a reboot wait time.

Use the **undo schedule reboot** command to disable the scheduled reboot function.

By default, the scheduled reboot function is disabled.

Note that:

- The reboot wait time can be in the format of hh:mm (hours:minutes) or mm (absolute minutes). The absolute minutes cannot exceed 30 x 24 x 60 minutes, namely, 30 days.
- The precision of the device timer is 1 minute. One minute before the reboot time, the device will prompt “REBOOT IN ONE MINUTE” and will be rebooted in one minute.

- After you execute the above command, the device will prompt you to confirm the configuration. You must enter <Y> or <y> to make the configuration take effect. The original configuration will be overwritten at the same time.
- If you use the **clock** command after the **schedule reboot delay** command to adjust the system time, the reboot wait time set by the **schedule reboot delay** command will become invalid.
- If you are performing file operations when the device is to be rebooted, the system does not execute the command for the sake of security.

Caution

This command reboots the device after the specified delay time, thus resulting in service interruption. Please use it with caution.

Examples

Configure the device to reboot in 88 minutes (supposing the current time is 11:48).

```
<Sysname> schedule reboot delay 88
Reboot system at 13:16 06/06/2006(in 1 hour(s) and 28 minute(s)). confirm? [Y/N]:
```

If you have used the **terminal logging** command to enable the log display function on the terminal before setting a reboot time, the system will automatically display related log information after you enter **y.** By default, the log display function is enabled on the terminal.

```
<Sysname>
%Jun  6 11:48:44:860 2006 Sysname CMD/4/REBOOT:
vty0(192.168.1.54): Set schedule reboot parameters at 11:48:44 06/06/2006, and system will
reboot at 13:16 06/06/2006.
```

shutdown-interval

Syntax

shutdown-interval *time*

undo shutdown-interval

View

System view

Default Level

2: System level

Parameters

time: Detection interval in seconds, in the range of 1 to 300.

Description

Use the **shutdown-interval** command to set a detection interval.

Use the **undo shutdown-interval** command to restore the default.

By default, the detection interval is 30 seconds.

Note that:

- If a protocol module such as the operation, administration and maintenance (OAM) module detects an exception on a port (for example, signal loss of the link on the peer end), the port will be closed automatically, without execution of the **shutdown** command. You can set the automatic recovery time of the port by using the **shutdown-interval** command.
- The **shutdown-interval** command helps you to dynamically set a detection interval to cooperate with the OAM module.
- If you change the detection interval to T1 during interface detection, the interval from when you change the interval to the time when detection starts is T. If T<T1, the interface which is down will be brought up after T1-T time; if T>=T1, the interface which is down will be brought up immediately.

Examples

Set the detection interval to 100 seconds.

```
<Sysname> system-view
[Sysname] shutdown-interval 100
```

startup bootrom-access enable

Syntax

startup bootrom-access enable

undo startup bootrom-access enable

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **startup bootrom-access enable** command to enable Boot ROM access during system startup (that is, you can press **Ctrl+B** to enter the Boot ROM menu).

Use the **undo startup bootrom-access enable** command to disable Boot ROM access during system startup (that is, you cannot enter the Boot ROM menu no matter whether you press **Ctrl+B** or not).

By default, Boot ROM access during system startup is enabled.

Refer to the **display startup** command in *File System Management Command*s in the *System Volume* for the related configuration.

Examples

Disable Boot ROM access during system startup.

```
<Sysname> undo startup bootrom-access enable
```

system-failure

Syntax

system-failure { **maintain** | **reboot** }

undo system-failure { **maintain** | **reboot** }

View

System view

Default Level

3: Manage level

Parameters

maintain: Specifies that when the system detects any software abnormality, it maintains the current situation, and does not take any measure to recover itself.

reboot: Specifies that when the system detects any software abnormality, it recovers itself through automatic reboot.

Description

Use the **system-failure** command to configure the exception handling method on all member devices.

By default, all member devices adopt the **reboot** method to handle exceptions.

The exception handling method is effective to the failed member device only, and does not influence the operations of other IRF members

Examples

Set the exception handling method to **reboot**.

```
<Sysname> system-view
[Sysname] system-failure reboot
```

5 File System Management Commands

Note

- The current working directory is the root directory of the storage medium on the device in the examples in this manual.
- For the qualified filename formats, refer to *File System Management Configuration* in the *System Volume*.

File System Configuration Commands

cd

Syntax

cd { *directory* | **..** | ***/*** }

View

User view

Default Level

3: Manage level

Parameters

directory: Name of the target directory, in the format of [*drive*:][*/*]*path*. *drive* represents the name of the storage medium, which is flash for the switch 4210G s not specified, it indicates the file or subfolder under the current directory.

..: Returns to the upper directory. If the current working directory is the root directory, or there is no such an upper directory, the current working directory is not changed after the execution of the **cd** command. No command line help for this keyword.

/: Returns to the root directory of the storage medium. No command line help for this keyword.

Description

Use the **cd** command to change the current working directory.

Examples

Enter the **test** folder after logging in to the device.

```
<Sysname> cd test
```

Return to the upper directory (Remember to enter a space after the keyword **cd**).

```
<Sysname> cd ..
```

Return to the root directory.

```
<Sysname> cd /
```

Enter the root directory of the flash on a slave with the member ID 2 after logging in to the master.

```
<Sysname> cd slot2#flash:/
```

Change the current directory from the file system of the slave to the **test** folder under the root directory of the master.

```
<Sysname> cd flash:/test
```

copy

Syntax

copy *fileurl-source fileurl-dest*

View

User view

Default Level

3: Manage level

Parameters

fileurl-source: Name of the source file.

fileurl-dest: Name of the target file or folder.

Description

Use the **copy** command to copy a file.

If you specify a target folder, the system will copy the file to the specified folder and use the name of the source file as the file name.

Examples

Copy file **testcfg.cfg** under the current folder and save it as **testbackup.cfg**.

```
<Sysname> copy testcfg.cfg testbackup.cfg
Copy flash:/test.cfg to flash:/testbackup.cfg?[Y/N]:y
....
%Copy file flash:/test.cfg to flash:/testbackup.cfg...Done.
```

After logging in to the master, copy the configuration file of the master to the root directory of a slave (with the member ID 2).

```
<Sysname> copy vrcfg.cfg slot2#flash:/
Copy flash:/vrcfg.cfg to slot2#flash:/vrcfg.cfg?[Y/N]:y

%Copy file flash:/vrcfg.cfg to slot2#flash:/vrcfg.cfg...Done.
```

delete

Syntax

delete [/**unreserved**] *file-url*

View

User view

Default Level

3: Manage level

Parameters

/**unreserved**: Permanently deletes the specified file, and the deleted file can never be restored.

file-url: Name of the file to be deleted. Asterisks (*) are acceptable as wildcards. For example, to remove files with the extension of **.txt** in the current directory, you may use the **delete ***.txt command.

Description

Use the **delete** command to move a specified file from a storage medium to the recycle bin, where you can restore the file with the **undelete** command or permanently delete it with the **reset recycle-bin** command.

The **dir /all** command can display the files moved to the recycle bin. These files are enclosed in pairs of brackets.

 **Caution**

If you delete two files in different directories but with the same filename, only the last one is retained in the recycle bin.

Examples

Remove file **tt.cfg** from the root directory of the storage medium on the master after logging in to the device.

```
<Sysname> delete tt.cfg
.
Delete flash:/tt.cfg?[Y/N]:y
.
%Delete file flash:/tt.cfg...Done.
```

Remove file **tt.cfg** from the root directory of the storage medium on a slave (with the member ID 2) after logging in to the device.

- Method 1

```
<Sysname> delete slot2#flash:/tt.cfg
Delete slot2#flash:/tt.cfg?[Y/N]:y
%Delete file slot2#flash:/tt.cfg...Done.
```

- Method 2

```
<Sysname> cd slot2#flash:/
<Sysname> delete tt.cfg
Delete slot2#flash:/tt.cfg?[Y/N]:y
%Delete file slot2#flash:/tt.cfg...Done.
```

dir

Syntax

dir [**/all**] [*file-url*]

View

User view

Default Level

3: Manage level

Parameters

/all: Displays all files (including those in the recycle bin).

file-url: Name of the file or directory to be displayed. Asterisks (*) are acceptable as wildcards. For example, to display files with the **.txt** extension under the current directory, you may use the **dir ***.txt command.

Description

Use the **dir** command to display information about all visible files and folders in the current directory.

Use the **dir /all** command to display information about all files and folders in the current directory, including hidden files, hidden sub-folders and the files in the recycle bin that originally belong to the current directory. The names of these deleted files are enclosed in pairs of brackets [ ].

The **dir** *file-url* command displays information about a file or folder.

Examples

Display information about all files and folders in the storage medium of the master after logging in to the device.

```
<Sysname> dir /all
Directory of flash:/

  0    -rwh        4  Apr 26 2008 12:02:05   snmpboots
  1    -rw-  10187730  Apr 26 2008 16:47:07   startup.bin
  2    -rwh     3144  Apr 26 2008 13:45:35   private-data.txt
  3    -rw-     2161  Apr 26 2008 13:53:25   startup.cfg
  4    -rw-  10058752  Sep 19 2008 17:41:46   startup_b58.bin
  5    -rw-  10139143  Apr 26 2008 13:08:20   startup_wenxiangchong.bin
  6    -rwh      716  Apr 26 2008 12:01:58   hostkey
  7    -rwh      572  Apr 26 2008 12:02:11   serverkey
  8    -rwh      548  Apr 26 2008 12:02:17   dsakey
  9    -rw-     3035  Apr 26 2008 13:45:42   new-config.cfg
  10   -rw-     2200  Apr 26 2008 14:58:35   [aa.cfg]
```

```
31496 KB total (1801 KB free)
```

Display information about all files and folders in the storage medium of a slave (with the member ID 2) after logging in to the device.

```
<Sysname> cd slot2#flash:/
<IRF>dir /all
Directory of slot2#flash:/

   0     -rwh     3144  Apr 26 2008 13:45:28   private-data.txt
   1     -rw-     2341  Apr 26 2008 16:36:18   startup.cfg
   2     -rw-      124  Apr 26 2008 12:00:22   patchstate
   3     -rwh      716  Apr 26 2008 14:31:36   hostkey
   4     -rwh        4  Apr 26 2008 14:31:41   snmpboots
   5     -rw-  10187730  Apr 26 2008 12:01:10   startup.bin
   6     -rwh      572  Apr 26 2008 14:31:47   serverkey
   7     -rwh      548  Apr 26 2008 14:31:52   dsakey
   8     -rw-     3035  Apr 26 2008 13:45:36   new-config.cfg
   9     drw-        -  Apr 26 2008 12:11:53   oldver

31496 KB total (1839 KB free)
```

Table 5-1 dir command output description

Field	Description
Directory of	The current working directory
d	Directory. If it is not displayed, it indicates that the displayed item is a file.
r	The directory or file is readable.
w	The directory or file is writeable.
h	The directory or file is hidden.
[ ]	The file is in the recycle bin.

execute

Syntax

execute *filename*

View

System view

Default Level

2: System level

Parameters

filename: Name of a batch file with a .bat extension. You can use the **rename** command to change the suffix of the configuration file to .bat to use it as a batch file.

Description

Use the **execute** command to execute the specified batch file.

Batch files are command line files. Executing a batch file is to execute a set of command lines in the file.

- You should not include invisible characters in a batch file. If an invisible character is found during the execution, the batch process will abort and the commands that have been executed cannot be cancelled.
- Not every command in a batch file is sure to be executed. For example, if a certain command is not correctly configured, the system omits this command and goes to the next one.
- The configuration generated after a batch file is executed will not be backed up to the standby main board automatically.
- Each configuration command in a batch file must be a standard configuration command, meaning that the valid configuration information can be displayed with the **display current-configuration** command after this command is configured successfully; otherwise, this command may not be executed correctly.

Examples

Execute the batch file **test.bat** in the root directory.

```
<Sysname> system-view
[Sysname] execute test.bat
```

file prompt

Syntax

file prompt { **alert** | **quiet** }

View

System view

Default Level

3: Manage level

Parameters

alert: Enables the system to warn you about operations that may bring undesirable results such as file corruption or data loss.

quiet: Disables the system from warning you about any operation.

Description

Use the **file prompt** command to set a prompt mode for file operations.

By default, the prompt mode is **alert**.

Note that when the prompt mode is set to **quiet**, the system does not warn for any file operation. To avoid undesirable consequences resulting from misoperation, you are recommended to use the **alert** mode.

Examples

Set the file operation prompt mode to **alert**.

```
<Sysname> system-view
[Sysname] file prompt alert
```

fixdisk

Syntax

fixdisk *device*

View

User view

Default Level

3: Manage level

Parameters

device: Storage medium name.

Description

Use the **fixdisk** command to restore the space of a storage medium when it becomes unavailable because of some abnormal operation.

Note that you can execute the **fixdisk** command for the storage medium on the master, but you cannot execute the command for the storage medium on the slaves.

Examples

Restore the space of the flash.

```
<Sysname> fixdisk flash:
Fixdisk flash: may take some time to complete...
%Fixdisk flash: completed.
```

format

Syntax

format *device*

View

User view

Default Level

3: Manage level

Parameters

device: Name of a storage medium.

Description

Use the **format** command to format a storage medium.

Caution

Formatting a storage medium results in loss of all the files on the storage medium and these files cannot be restored. In particular, if there is a startup configuration file on a storage medium, formatting the storage medium results in loss of the startup configuration file.

Examples

Format the flash.

```
<Sysname> format flash:
All data on flash: will be lost, proceed with format? [Y/N]:y
./
%Format flash: completed.
```

mkdir

Syntax

mkdir *directory*

View

User view

Default Level

3: Manage level

Parameters

directory: Name of a folder.

Description

Use the **mkdir** command to create a folder under a specified directory on the storage medium.

Note that:

- The name of the folder to be created must be unique under the specified directory. Otherwise, you will fail to create the folder under the directory.
- To use this command to create a folder, the specified directory must exist. For instance, to create folder **flash:/test/mytest**, the **test** folder must exist. Otherwise, you will fail to create folder **mytest**.

Examples

Create a folder named **test** under the current directory.

```
<Sysname> mkdir test
....
%Created dir flash:/test
```

Create folder **test/subtest** under the current directory.

```
<Sysname> mkdir test/subtest
....
```

```
%Created dir flash:/test/subtest
```

Create folder **test** on a slave (with the member ID 2) after logging in to the device.

```
<Sysname> mkdir slot2#flash:/test
....
%Created dir slot2#flash:/test.
```

more

Syntax

more *file-url*

View

User view

Default Level

3: Manage level

Parameters

file-url: File name.

Description

Use the **more** command to display the contents of the specified file.

So far, this command is valid only for text files.

Examples

Display the contents of file **test.txt**.

```
<Sysname> more test.txt
Welcome to 4210G
```

Display the contents of file **testcfg.cfg**.

```
<Sysname> more testcfg.cfg

#
 version 5.20, ESS 2201
#
 sysname Sysname
#
vlan 2
#
return
<Sysname>
```

Display the contents of file **testcfg.cfg** on a slave (with the member ID 2).

```
<Sysname> more slot2#flash:/testcfg.cfg

#
 version 5.20, ESS 2201
#
```

```
 sysname Test
#
  ---- More ----
```

move

Syntax

move *fileurl-source fileurl-dest*

View

User view

Default Level

3: Manage level

Parameters

fileurl-source: Name of the source file.

fileurl-dest: Name of the target file or folder.

Description

Use the **move** command to move a file.

If you specify a target folder, the system will move the source file to the specified folder, with the file name unchanged.

Examples

Move file **flash:/test/sample.txt** to **flash:/**, and save it as **1.txt**.

```
<Sysname> move test/sample.txt 1.txt
Move flash:/test/sample.txt to flash:/1.txt?[Y/N]:y
...
% Moved file flash:/test/sample.txt to flash:/1.txt
```

Move file **b.cfg** to the subfolder **test2**.

```
<Sysname> move b.cfg test2
Move flash:/b.cfg to flash:/test2/b.cfg?[Y/N]:y
.
%Moved file flash:/b.cfg to flash:/test2/b.cfg.
```

pwd

Syntax

pwd

View

User view

Default Level

3: Manage level

Parameters

None

Description

Use the **pwd** command to display the current path.

Examples

Display the current path.

```
<Sysname> pwd
flash:
```

rename

Syntax

rename *fileurl-source fileurl-dest*

View

User view

Default Level

3: Manage level

Parameters

fileurl-source: Name of the source file or folder.

fileurl-dest: Name of the target file or folder.

Description

Use the **rename** command to rename a file or folder.

The target file name must be unique under the current path.

Examples

Rename file **sample.txt** as **sample.bat**.

```
<Sysname> rename sample.txt sample.bat
Rename flash:/sample.txt to flash:/sample.bat? [Y/N]:y

% Renamed file flash:/sample.txt to flash:/sample.bat
```

reset recycle-bin

Syntax

reset recycle-bin [**/force**]

View

User view

Default Level

3: Manage level

Parameters

/force: Deletes all files in the recycle bin, including files that cannot be deleted by the command without the **/force** keyword.

Description

Use the **reset recycle-bin** command to permanently delete the files in the recycle bin in the current directory.

If a file is corrupted, you may not be able to delete the file using the **reset recycle-bin** command. In this case, you can use the **reset recycle-bin /force** command, which can delete all the files in the recycle bin forcibly.

Note that:

- Unlike this command, the **delete** *file-url* command only moves a file to the recycle bin, and the file still occupies the memory space. To delete the file in the recycle bin, you need to execute the **reset recycle-bin** command in the original directory of the file.
- The **reset recycle-bin** command deletes files in the current directory and in the recycle bin. If the original path of the file to be deleted is not the current directory, use the **cd** command to enter the original directory of the file, and then execute the **reset recycle-bin** command.

Examples

Delete file **b.cfg** under the current directory and in the recycle bin.

- Display all the files in the recycle bin and under the current directory.

```
<Sysname> dir /all

Directory of flash:/

  0     -rw-  10471471  Sep 18 2008 02:45:15   4210G.bin
  1     -rwh        4  Apr 26 2000 12:03:51   snmpboots
  2     -rwh     1792  Apr 26 2000 12:49:53   private-data.txt
  3     -rw-  9989823  Jul 14 2008 19:30:46   4210G_b57.bin
  4     -rw-        6  Apr 26 2000 12:04:33   patchstate
  5     -rw-     2209  Apr 26 2000 12:07:20   startup.cfg
  6     -rwh      716  Apr 26 2000 12:03:46   hostkey
  7     -rwh      572  Apr 26 2000 12:03:55   serverkey
  8     -rwh      548  Apr 26 2000 12:04:00   dsakey
  9     -rw-   478164  Apr 26 2000 14:52:35   4210G_505.btm
  10    -rw-      368  Apr 26 2000 12:04:04   patch_xxx.bin
  11    -rw-     2195  Apr 26 2000 12:43:08   sfp.cfg
  12    -rw-     5501  Apr 26 2000 13:05:57   [a.cfg]
  13    -rw-     2159  Apr 26 2000 13:06:04   [b.cfg]

31496 KB total (11018 KB free)
```

*//The above information indicates that the current directory is **flash:**, and there are two files **a.cfg** and **b.cfg** in the recycle bin.*

- Delete file **b.cfg** under the current directory and in the recycle bin.

```
<Sysname> reset recycle-bin
Clear flash:/~/a.cfg ?[Y/N]:n
Clear flash:/~/b.cfg ?[Y/N]:y
Clearing files from flash may take a long time. Please wait...
......
%Cleared file flash:/~/b.cfg...
```

- In directory **flash:**, check whether the file **b.cfg** in the recycle bin is deleted.

```
<Sysname> dir /all

Directory of flash:/

   0    -rw-  10471471  Sep 18 2008 02:45:15   4210G-d501.bin
   1    -rwh        4  Apr 26 2000 12:03:51   snmpboots
   2    -rwh     1792  Apr 26 2000 12:49:53   private-data.txt
   3    -rw-   9989823  Jul 14 2008 19:30:46   4210G_b57.bin
   4    -rw-        6  Apr 26 2000 12:04:33   patchstate
   5    -rw-     2209  Apr 26 2000 12:07:20   startup.cfg
   6    -rwh      716  Apr 26 2000 12:03:46   hostkey
   7    -rwh      572  Apr 26 2000 12:03:55   serverkey
   8    -rwh      548  Apr 26 2000 12:04:00   dsakey
   9    -rw-   478164  Apr 26 2000 14:52:35   4210G_505.btm
   10   -rw-      368  Apr 26 2000 12:04:04   patch_xxx.bin
   11   -rw-     2195  Apr 26 2000 12:43:08   sfp.cfg
   12   -rw-     2195  Apr 26 2000 13:08:47   [a.cfg]

31496 KB total (11015 KB free)
```

*// The above information indicates that file **flash:/b.cfg** is deleted permanently.*

Delete file **aa.cfg** in the subdirectory **test** and in the recycle bin.

- Enter the subdirectory

```
<Sysname> cd test/
```

- Check all the files in the subfolder **test**.

```
<Sysname> dir /all
Directory of flash:/test

   0    -rw-     2195  Apr 26 2000 21:22:35   [aa.cfg]

31496 KB total (11010 KB free)
```

// The above information indicates only one file exists in the folder, and the file has been moved to the recycle bin.

- Permanently delete file **test/aa.cfg**.

```
<Sysname> reset recycle-bin
Clear flash:/test/~/aa.cfg ?[Y/N]:y
Clearing files from flash may take a long time. Please wait...
..
%Cleared file flash:/test/~/aa.cfg...
```

rmdir

Syntax

rmdir *directory*

View

User view

Default Level

3: Manage level

Parameters

directory: Name of the folder.

Description

Use the **rmdir** command to remove a folder.

- The folder must be an empty one. If not, you need to delete all files and subfolders under it with the **delete** command.
- After you execute the **rmdir** command successfully, the files in the recycle bin under the folder will be automatically deleted.

Examples

Remove folder **mydir**.

```
<Sysname> rmdir mydir
Rmdir flash:/mydir?[Y/N]:y

%Removed directory flash:/mydir.
```

undelete

Syntax

undelete *file-url*

View

User view

Default Level

3: Manage level

Parameters

file-url: Name of the file to be restored.

Description

Use the **undelete** command to restore a file from the recycle bin.

If another file with the same name exists under the same path, the undelete operation will cause it to be overwritten and the system will prompt you whether to continue.

Examples

Restore file **a.cfg** in directory **flash:** from the recycle bin.

```
<Sysname> undelete a.cfg
Undelete flash:/a.cfg?[Y/N]:y
.....
%Undeleted file flash:/a.cfg.
```

Restore file **b.cfg** in directory **flash:/test** from the recycle bin.

```
<Sysname> undelete flash:/test/b.cfg
Undelete flash:/test/b.cfg?[Y/N]:y
.......
%Undeleted file flash:/test/b.cfg.
```

Or, you can use the following steps to restore file **flash:/test/b.cfg**.

```
<Sysname> cd test
<Sysname> undelete b.cfg
Undelete flash:/test/b.cfg?[Y/N]:y
.....
%Undeleted file flash:/test/b.cfg.
```

Configuration File Management Commands

archive configuration

Syntax

archive configuration

View

User view

Default Level

3: Manage level

Parameters

None

Description

Use the **archive configuration** command to save the current running configuration manually.

After the execution of this command, the system saves the current running configuration with the specified filename (filename prefix + serial number) to the specified path.

Note the following:

- Before executing the **archive configuration** command, you must configure the filename prefix and path of the saved configuration file by using the **archive configuration location** command.
- After execution of the **archive configuration** command, the current running configuration is only saved to the master, and the slaves do not perform the saving operation.

Examples

Save the current running configuration manually.

```
<Sysname> archive configuration
Warning: Save the running configuration to an archive file. Continue? [Y/N]: Y
Please wait...
Info: The archive configuration file myarchive_1.cfg is saved.
```

archive configuration interval

Syntax

archive configuration interval *minutes*

undo archive configuration interval

View

System view

Default Level

3: Manage level

Parameters

minutes: Specifies the interval for automatically saving the current running configuration, in minutes. The value ranges from 10 to 525,600 (365 days).

Description

Use the **archive configuration interval** command to enable the automatic saving of the current running configuration and set the interval.

Use the **undo archive configuration interval** command to restore the default.

By default, the system does not save the current running configuration automatically.

After the execution of this command, the system saves the current running configuration with the specified filename to the specified path at a specified interval (the value of the *minutes* argument).

Configure an automatic saving interval according to the storage medium performance and the frequency of configuration modification:

- If the configuration of the device does not change frequently, you are recommended to save the current running configuration manually as needed
- If a low-speed storage medium (such as a flash) is used, you are recommended either to save the current running configuration manually, or to configure automatic saving with an interval longer than 1,440 minutes (24 hours).

Note the following:

- Before executing the **archive configuration interval** command, you must configure the filename prefix and path of the saved configuration file by using the **archive configuration location** command.
- After execution of the **archive configuration interval** command, the current running configuration is only saved to the master, and the slaves cannot save the configuration. However, the command is executed on both the master and the slaves to ensure the rollback of the configuration after the master is changed.

Examples

Configure the system to save the current running configuration every 60 minutes.

```
<Sysname> system-view
[Sysname] archive configuraion interval 60
Info: Archive files will be saved every 60 minutes.
```

archive configuration location

Syntax

archive configuration location *directory* **filename-prefix** *filename-prefix*

undo archive configuration location

View

System view

Default Level

3: Manage level

Parameters

directory: The path of the folder for saving the saved configuration file, a case insensitive string of 1 to 63 characters, in the format of storage medium name:/[folder name]/subfolder name. The folder must be created before the configuration.

filename-prefix: The filename prefix of a saved configuration file, a case insensitive string of 1 to 30 characters (can include letters, numbers, _, and - only).

Description

Use the **archive configuration location** command to configure the path and filename prefix of a saved configuration file.

Use the **undo archive configuration location** command to restore the default.

By default, the path and filename prefix of a saved configuration file are not configured, and the system does not save the configuration file periodically.

Note the following:

- Before the current running configuration is saved either manually or automatically, the file path and filename prefix must be configured.
- If the **undo archive configuration location** command is executed, the current running configuration can neither be saved manually nor automatically, and the configuration by executing the **archive configuration interval** and **archive configuration max** commands restores to the default, meanwhile, the saved configuration files are cleared.
- The saving and rollback operations are executed only on the master. To make the configuration rollback take effect on the new master after an active/standby switchover, execute the **archive configuration location** command to specify the path and filename prefix of the saved configuration file on both the master and slaves. Therefore, before the execution of this command, ensure that the specified path is available on both the master and the slaves, and the path cannot include any member ID.

Examples

Configure the path and the filename prefix of a saved configuration file as **flash:/archive/** and **my_archive** respectively.

- Create folder **flash:/archive** on the master.

```
<Sysname> mkdir archive
.
%Created dir flash:/archive.
```

- Create folder **flash:/archive** on a slave (with the member ID 2).

```
<Sysname> mkdir slot2#flash:/archive

%Created dir slot2#flash:/archive.
```

- Configure the path and the filename prefix of the saved configuration file.

```
<Sysname> system-view
[Sysname] archive configuration location flash:/archive filename-prefix my_archive
```

archive configuration max

Syntax

archive configuration max *file-number*

undo archive configuration max

View

System view

Default Level

3: Manage level

Parameters

file-number: The maximum number of configuration files that can be saved, in the range 1 to 10. The value of the *file-number* argument is determined by the memory space. You are recommended to set a comparatively small value for this argument if the available memory space is small.

Description

Use the **archive configuration max** command to set the maximum number of configuration files that can be saved.

Use the **undo archive configuration max** command to restore the default.

By default, a maximum of 5 configuration files can be saved.

Since excessive configuration files occupy large memory space, you can use this command to control the number of the files. After the maximum number of configuration files is saved, the system deletes the oldest files when the next file is saved (either automatically or manually). When you change the maximum number of configuration files that can be saved, the exceeded files are not deleted. If the number of the existing configuration files is larger than or equal to the newly configured upper limit, the system deletes the oldest *n* files when the next file is saved, where n = the current number - the newly configured number + 1, for example: if the number of configuration files that have been saved is 7, and the newly configured upper limit is 4, when there is a new configuration file to be saved, the system deletes 4 oldest files, where 4 = 7-4+1.

Before executing this command, configure the path and filename prefix of a saved configuration file by using the **archive configuration location** command; otherwise, the execution of this command fails.

Note that, if the **undo archive configuration location** command is executed, the maximum number of configuration files that can be saved also restores to the default.

Examples

Set the maximum number of configuration files that can be saved to 10.

```
<Sysname> system-view
[Sysname] archive configuration max 10
```

backup startup-configuration

Syntax

backup startup-configuration to *dest-addr* [*dest-filename*]

View

User view

Default Level

2: System level

Parameters

dest-addr: IP address or name of a TFTP server. The address cannot be an IPv6 address.

dest-filename: Target filename used to save the startup configuration file for the next system startup on the server.

Description

Use the **backup startup-configuration** command to back up the startup configuration file (used at the next system startup) to a specified TFTP server. If you do not specify this filename, the original filename is used.

For a device that has main and backup startup configuration files, this command only backs up the main startup configuration file.

Presently, the device uses TFTP to back up configuration files.

Examples

Back up the startup configuration file of the device to the TFTP server with IP address 2.2.2.2, using filename **192-168-1-26.cfg**.

```
<Sysname> display startup
  Current startup saved-configuration file: flash:/sfp.cfg
  Next main startup saved-configuration file: flash:/sfp.cfg
  Next backup startup saved-configuration file: NULL
<Sysname> backup startup-configuration to 2.2.2.2 192-168-1-26.cfg
Backup next startup-configuration file to 2.2.2.2, please wait…finished!
<Sysname>
```

After the above operation, the device backs up file **sfp.cfg** to TFTP server 2.2.2.2, where the file is saved as **192-168-1-26.cfg**.

configuration replace file

Syntax

configuration replace file *filename*

View

System view

Default Level

3: Manage level

Parameters

filename: Specifies the name of the replacement configuration file for configuration rollback.

Description

Use the **configuration replace file** command to set configuration rollback.

After the execution of this command, the current running configuration rolls back to the configuration state based on the specified configuration file (*filename*).

Examples

Roll back from the current running configuration to a previous configuration state based on a saved configuration file **my_archive_1.cfg**.

```
<Sysname> system-view
[Sysname] configuration replace file my_archive_1.cfg
Info: Now replacing the current configuration. Please wait...
Info: Succeeded in replacing current configuration with the file my_archive_1.cfg.
```

display archive configuration

Syntax

display archive configuration

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display archive configuration** command to display the information about configuration rollback.

Examples

Display the information about configuration rollback.

```
<Sysname> display archive configuration
Location: flash:/archive
Filename prefix: my_archive
Archive interval in minutes: 120
Maximum number of archive files: 10
Saved archive files:
  No. TimeStamp            FileName
  1   Aug 05 2007 20:24:54   my_archive_1.cfg
  2   Aug 05 2007 20:34:54   my_archive_2.cfg
# 3   Aug 05 2007 20:44:54   my_archive_3.cfg
'#' indicates the most recent archive file.
Next archive file to be saved: my_archive_4.cfg
```

Table 5-2 display archive configuration command output description

Field	Description
Location	Absolute path of the saved configuration files
Archive interval in minutes	Configuration file saving interval, in minutes. If the automatic saving is disabled, this field is not displayed.

display saved-configuration

Syntax

display saved-configuration [**by-linenum**]

View

Any view

Default Level

2: System level

Parameters

by-linenum: Identifies each line of displayed information with a line number.

Description

Use the **display saved-configuration** command to display the contents of the configuration file saved for the next startup of the device.

During device management and maintenance, you can use this command to check whether important configurations are saved to the configuration file to be used for the next startup of the device.

This command displays the main configuration file to be used for the next system startup.

If the system is not specified with a configuration file for the next startup or the specified configuration file does not exist, no information will be displayed when you execute the **display saved-configuration** command.

Related commands: **save**, **reset saved-configuration**; **display current-configuration** in *Basic System Configuration Commands* in the *System Volume*.

Examples

Display the configuration file saved for the next startup of the device.

```
<Sysname> display saved-configuration
#
 version 5.20, ESS 2201
#
 sysname Sysname
#
 domain default enable system
#
 telnet server enable
#
 multicast routing-enable
#
vlan 1
#
vlan 999
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
interface NULL0
#
  ---- More ----
```

The configurations are displayed in the order of global, port, and user interface. “ ---- More ----” means that all information on this screen has been displayed, and if you press the Space key, the next screen will be displayed.

Display the contents of the configuration file saved for the next startup of the device with a number identifying each line.

```
<Sysname> display saved-configuration by-linenum
    1:  #
    2:   version 5.20, ESS 2201
    3:  #
    4:   sysname Sysname
    5:  #
    6:   domain default enable system
    7:  #
    8:   telnet server enable
    9:  #
   10:   multicast routing-enable
   11:  #
   12:  vlan 1
   13:  #
```

```
 14:  vlan 999
 15:  #
 16:  domain system
 17:   access-limit disable
 18:   state active
 19:   idle-cut disable
 20:   self-service-url disable
 21:  #
 22:  interface NULL0
 23:  #
---- More ----
```

“ ---- More ----” means that all information on this screen has been displayed, and if you press the Space key, the next screen will be displayed.

display startup

Syntax

display startup

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display startup** command to display the configuration files used at the current system startup and the configuration file(s) to be used at the next system startup.

Note that:

- The slaves are started and run based on the current configurations of the master; therefore the current startup configuration files displayed on all the member devices in a IRF are always the same.
- After the master is changed, the new master does not restart using the configuration file but runs with the current configuration instead. Therefore, when you execute the **display startup** command, the startup configuration file used for the current startup of the new master is displayed as NULL and those of the slaves are also NULL to keep consistent with the new master.

Related commands: **startup saved-configuration**.

Examples

Display the startup configuration file used at the current system startup and the one to be used at the next system startup.

```
<Sysname> display startup
MainBoard:
```

```
 Current startup saved-configuration file: NULL
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: flash:/startup2.cfg
Slot 2:
 Current startup saved-configuration file: NULL
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: flash:/startup2.cfg
```

Table 5-3 display startup command output description

Field	Description
MainBoard	The configuration files used for the current and the next startup of the master
Current Startup saved-configuration file	The configuration file used for the current startup
Next main startup saved-configuration file	The main configuration file used for the next startup
Next backup startup saved-configuration file	The backup configuration file used for the next startup
Slot 2	The configuration files used for the current and the next startup of the slave (with the member ID 2)

reset saved-configuration

Syntax

reset saved-configuration [**backup** | **main**]

View

User view

Default Level

2: System level

Parameters

backup: Deletes the backup startup configuration file.

main: Deletes the main startup configuration file.

Description

Use the **reset saved-configuration** command to delete the startup configuration file saved on the storage medium of the device.

Note that:

- This command will permanently delete the configuration file from all the member devices in a IRF. Use it with caution.
- On a device that has the main and backup startup configuration files, you can choose to delete either the main or backup startup configuration file. However, in the case that the main and backup startup configuration files are the same, if you perform the delete operation for once, the

system will not delete the configuration file but only set the corresponding startup configuration file (main or backup, according to which one you specified in the command) to NULL.

- The execution of the **reset saved-configuration** command and that of the **reset saved-configuration main** command have the same effect, that is, they will delete the main startup configuration file.

Related commands: **save**, **display saved-configuration**.

Examples

Delete the startup configuration file for the next startup from the storage medium of the device.

```
<Sysname> reset saved-configuration backup
The saved configuration file will be erased. Are you sure? [Y/N]:y
Configuration file in flash is being cleared.
Please wait ...
..
MainBoard:
 Configuration file is cleared.
Slot 2:
 Erase next configuration file successfully
```

restore startup-configuration

Syntax

restore startup-configuration from *src-addr src-filename*

View

User view

Default Level

2: System level

Parameters

src-addr: IP address or name of a TFTP server. The address cannot be an IPv6 address.

src-filename: Filename of the configuration file to be downloaded from the specified server.

Description

Use the **restore startup-configuration** command to download a configuration file from the specified TFTP server to the device and specify the configuration file as the startup configuration file to be used at the next startup of the device.

- The file downloaded is set as the main startup configuration file to be used at the next system startup.
- This command downloads the configuration file to the root directory of the storage medium of all the member devices and specifies the file as the startup configuration file to be used at the next startup of all the member devices.

If the file to be downloaded has the same filename as an existing file on a member device, you will be prompted whether you want to overwrite the existing file or not. In addition, both the master and the slaves are assumed to use the storage media of the same type when the device is checking the

filename or backing up the configuration file to the slaves. When backing up the configuration file to the slaves, the device saves the file to the same directory on the slaves as on the master, that is, the root directory.

Examples

Download file **config.cfg** from the TFTP server whose IP address is 2.2.2.2, and the file is to be used as the main configuration file at the next startup of the device.

```
<Sysname> restore startup-configuration from 2.2.2.2 config.cfg
Restore next startup-configuration file from 2.2.2.2. Please wait...finished!
Now restore next startup-configuration file from main to slave board. Please wait...finished!
```

save

Syntax

save *file-url* [**all** | **slot** *slot-number*]

save [**safely**] [**backup** | **main**]

View

Any view

Default Level

2: System level

Parameters

file-url: File path, where the extension of the file name must be .cfg. When used with the keyword **all** or **slot**, this argument cannot include a member ID. If the file path includes a folder name, you must first create the folder on the member device; otherwise, the operation will fail.

all: Saves the current configuration in the specified filename to all the member devices in a IRF.

slot *slot-number*: Saves the current configuration in the specified filename to a slave. *slot-number* represents the member ID of a member device. The value range depends on the device model. You can use the **display irf** command to view the member IDs of the member devices in a IRF.

safely: Sets the configuration saving mode to safe. If this argument is not specified, the configuration file is saved in fast mode.

backup: Saves the current configuration to the startup configuration file specified in the interactive mode, and specifies the file as the backup startup configuration file to be used at the next startup of the device.

main: Saves the current configuration to the main startup configuration file specified in the interactive mode, and specifies the file as the main startup configuration file to be used at the next startup of the device.

Description

Use the **save** *filename* [**all** | **slot** *slot-number*] command to save the current configuration to the specified configuration file, but the system will not specify the file as the startup configuration file for the next system startup. If the file specified by *filename* does not exist, the system will create the file and then save the configuration to the file; if the **all** or **slot** keyword is not specified, the configuration will be saved to the master.

Use the **save** [**safely**] [**backup** | **main**] command to save the current configuration to the root directory of the storage medium on a member device, and specify the file as the startup configuration file for the next system startup. If the **backup** or **main** keyword is not specified, the **main** keyword is used by default.

Whether the **save** [**safely**] [**backup** | **main**] command or the **save** *filename* **all** command+**Enter** takes effect on all the member devices or on the master only depends on whether the configuration file auto-save function is enabled.

Related commands: **slave auto-update config**, **reset saved-configuration**, **display current-configuration**, **display saved-configuration**.

Examples

Save the current configuration file to the specified directory, but do not specify the configuration file as the configuration file for the next startup.

```
<Sysname> save test.cfg
The current configuration will be saved to flash:/test.cfg. Continue? [Y/N]:y
Now saving current configuration to the device.
Saving configuration flash:/test.cfg. Please wait...
.............
Configuration is saved to flash successfully.
```

Save the current configuration to the root directory of the storage medium on a member device, and specify the file as the configuration file for the next startup.

```
<Sysname> display startup
MainBoard:
 Current startup saved-configuration file: NULL
 Next main startup saved-configuration file: flash:/aa.cfg
 Next backup startup saved-configuration file: NULL
Slot 2:
 Current startup saved-configuration file: NULL
 Next main startup saved-configuration file: flash:/aa.cfg
 Next backup startup saved-configuration file: NULL
```

*// The above information indicates that the main startup configuration file for the next startup of all the member devices is **aa.cfg**.*

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/aa.cfg]
(To leave the existing filename unchanged, press the enter key):startup.cfg
flash:/startup.cfg exists, overwrite? [Y/N]:y
 Validating file. Please wait..................
 Saved the current configuration to mainboard device successfully.
Slot 2:
 Save next configuration file successfully
 Configuration is saved to device successfully.
<Sysname> display startup
MainBoard:
 Current startup saved-configuration file: NULL
 Next main startup saved-configuration file: flash:/startup.cfg
```

```
 Next backup startup saved-configuration file: NULL
Slot 2:
 Current startup saved-configuration file: NULL
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: NULL
```

*// The above information indicates that the main configuration file for the next startup of all the member devices in the IRF is changed to **startup.cfg**.*

Save the current configuration in the name of **test.cfg** to a slave (with the member ID of 2) (approach 1).

```
<Sysname> save test.cfg slot 2
The current configuration will be saved to slot2#flash:/test.cfg. Continue? [Y/N]:y
Now saving current configuration to the device.
Saving configuration slot2#flash:/test.cfg. Please wait...
.........
Configuration is saved to slot2#flash successfully.
```

Or, you can use the following command (approach 2):

```
<Sysname> save slot2#flash:/test.cfg
```

slave auto-update config

Syntax

slave auto-update config

undo slave auto-update config

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **slave auto-update config** command to enable the configuration file auto-save function.

Use the **undo slave auto-update config** command to disable the function.

By default, the configuration file auto-save function is enabled.

Examples

Enable the configuration file auto-save function.

```
<Sysname> system-view
[Sysname] slave auto-update config
```

startup saved-configuration

Syntax

startup saved-configuration *cfgfile* [**backup** | **main**]

undo startup saved-configuration

View

User view

Default Level

2: System level

Parameters

cfgfile: Configuration file name. The file must be a file with an extension .cfg stored in the root directory of the storage medium.

backup: Sets the configuration file as the backup startup configuration file that will be used at the next startup of the device.

main: Sets the configuration file as the main startup configuration file that will be used at the next startup of the device.

Description

Use the **startup saved-configuration** command to specify a startup configuration file (the configuration file to be used at the next system startup) for all the member devices.

Use the **undo startup saved-configuration** command to configure all the member devices to start up with the null configuration, that is, the factory configuration.

The startup configuration file for the next startup of all the member devices must the same. Therefore, before using the command, ensure that the specified configuration file has been saved to the root directories of the storage media of all the member devices; otherwise, the command will fail.

- The **startup saved-configuration** and **startup saved-configuration main** commands have the same effect: Both of them are used to specify the main startup configuration file.
- The main and backup startup configuration files can be specified as the same file. However, it is recommended you use different files, or, save the same configuration as two files using different file names, one specified as the main startup configuration file, and the other specified as the backup.
- If you execute the **undo startup saved-configuration** command, the system will set the main and backup startup configuration file as NULL, but will not delete the two configuration files.

Related commands: **display startup**.

Examples

Specify a startup configuration file for the next system startup.

```
<Sysname> startup saved-configuration testcfg.cfg
Please wait ...
Setting the master board ..........
... Done!
Setting the slave board ...
```

```
Slot 2:
 Set next configuration file successfully
```

6 FTP Configuration Commands

FTP Server Configuration Commands

display ftp-server

Syntax

display ftp-server

View

Any view

Default Level

3: Manage level

Parameters

None

Description

Use the **display ftp-server** command to display the FTP server configuration.

After configuring FTP server parameters, you may verify them with this command.

Related commands: **ftp server enable**, **ftp timeout**, **ftp update**.

Examples

Display the FTP server configuration.

```
<Sysname> display ftp-server
  FTP server is running
  Max user number:            1
  User count:                1
  Timeout value(in minute):    30
  Put Method:                fast
```

Table 6-1 display ftp-server command output description

Field	Description
Max user number	Maximum number of login users at a time
User count	Number of the current login users
Timeout value (in minute)	Allowed idle time of an FTP connection. If there is no packet exchange between the FTP server and client during the whole period, the FTP connection will be disconnected.

Field	Description
Put Method	File update method of the FTP server, including: • fast: Fast update • normal: Normal update

display ftp-user

Syntax

display ftp-user

View

Any view

Default Level

3: Manage level

Parameters

None

Description

Use the **display ftp-user** command to display the detailed information of current FTP users.

Examples

Display the detailed information of FTP users.

```
<Sysname> display ftp-user
  UserName            HostIP    Port    Idle            HomeDir
      ftp       192.168.1.54    1190       0             flash:
```

If the name of the logged-in user exceeds 10 characters, the exceeded characters will be displayed in the next line and right justified, for example, if the logged-in user name is **administrator**, the information is displayed as follows:

```
<Sysname> display ftp-user
  UserName            HostIP    Port    Idle            HomeDir
administra
      tor      192.168.0.152    1031       0             flash:
```

Table 6-2 display ftp-user command output description

Field	Description
UserName	Name of the currently logged-in user
HostIP	IP address of the currently logged-in user
Port	Port which the currently logged-in user is using
Idle	Duration time of the current FTP connection, in minutes
HomeDir	Authorized path of the present logged-in user

free ftp user

Syntax

free ftp user *username*

View

User view

Default Level

3: Manage level

Parameters

username: Username. You can use the **display ftp-user** command to view the logged-in user name of the current FTP connection.

Description

Use the **free ftp user** command to manually release the FTP connection established with the specified username.

Note that if the user to be released is transmitting a file, the connection between the user and the FTP server is terminated after the file transmission.

Examples

Manually release the FTP connection established with username **ftpuser**.

```
<Sysname> free ftp user ftpuser
Are you sure to free FTP user ftpuser? [Y/N]:y
<Sysname>
```

ftp server acl

Syntax

ftp server acl *acl-number*

undo ftp server acl

View

System view

Default Level

3: Manage level

Parameters

acl-number: Basic access control list (ACL) number, in the range 2000 to 2999.

Description

Use the **ftp server acl** command to control the access to the device from FTP clients through ACL.

Use the **undo ftp server acl** command to restore the default.

By default, the access to the device from FTP clients is not controlled.

Associated with an ACL, the FTP server can deny the FTP requests of some FTP clients and only permit the access of clients allowed by the ACL rules. This configuration only filters the FTP connections to be established, and has no effect on the established FTP connections and operations. If you execute the command for multiple times, the last specified ACL takes effect.

Examples

Associate the FTP service with ACL 2001 to allow only the client 1.1.1.1 to access the device through FTP.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule 0 permit source 1.1.1.1 0
[Sysname-acl-basic-2001] rule 1 deny source any
[Sysname-acl-basic-2001] quit
[Sysname] ftp server acl 2001
```

ftp server enable

Syntax

ftp server enable

undo ftp server

View

System view

Default Level

3: Manage level

Parameters

None

Description

Use the **ftp server enable** command to enable the FTP server and allow the login of FTP users.

Use the **undo ftp server** command to disable the FTP server.

By default, the FTP server is disabled to prevent attacks.

Examples

Enable the FTP server.

```
<Sysname> system-view
[Sysname] ftp server enable
```

ftp timeout

Syntax

ftp timeout *minute*

undo ftp timeout

View

System view

Default Level

3: Manage level

Parameters

minute: Idle-timeout timer in minutes, in the range 1 to 35791.

Description

Use the **ftp timeout** command to set the idle-timeout timer.

Use the **undo ftp timeout** command to restore the default.

By default, the FTP idle time is 30 minutes.

After you log in to an FTP server, if the connection is disrupted and the FTP server is not notified, the system will maintain the connection, which will cause the occupation of the system resources and affect the login of other FTP users. To address this problem, you can set an idle-timeout timer so that the FTP server can disconnect from the user if no information is received or/and transmitted before the timer expires.

Examples

Set the idle-timeout timer to 36 minutes.

```
<Sysname> system-view
[Sysname] ftp timeout 36
```

ftp update

Syntax

ftp update { **fast** | **normal** }

undo ftp update

View

System view

Default Level

3: Manage level

Parameters

fast: Fast update.

normal: Normal update.

Description

Use the **ftp update** command to set the file update mode that the FTP server uses while receiving data.

Use the **undo ftp update** command to restore the default, namely, the normal mode.

Examples

Set the FTP update mode to **normal**.

```
<Sysname> system-view
[Sysname] ftp update normal
```

FTP Client Configuration Commands

Note

- In this section, the configuration procedure of entering FTP client view is omitted. You must use the **ftp** command to enter FTP client view for configurations under this view. For details, refer to ftp.
- Before executing the FTP client configuration commands in this section, make sure you have configured the proper authority for users on the FTP server, such as view the files under the current directory, read/download the specified file, create directory/upload files, rename/remove files, and so on.
- The prompt information in the examples of this section varies with FTP server types.

---

ascii

Syntax

ascii

View

FTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **ascii** command to set the file transfer mode to ASCII.

By default, the file transfer mode is ASCII.

The carriage return characters vary with operating systems. For example, to indicate the end of a line and transfer to the next line, the 3COM device system and Windows system use characters **/r/n**, and the Linux system uses characters **/n**. Therefore, after the file transmission between two systems that use different carriage return characters, such as Linux system and 3COM device system, the FTP transmission mode must be applied to ensure the correct resolution of the files.

FTP transfers files in two modes:

- Binary mode: for program file or picture transmission.

- ASCII mode: for text file transmission.

Related commands: **binary**.

Examples

Set the file transfer mode to ASCII.

```
[ftp] ascii
200 Type set to A.
```

binary

Syntax

binary

View

FTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **binary** command to set the file transfer mode to binary (also called flow mode).

By default, the transfer mode is ASCII mode.

Related commands: **ascii**.

Examples

Set the file transfer mode to **binary**.

```
[ftp] binary
200 Type set to I.
```

bye

Syntax

bye

View

FTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **bye** command to disconnect from the remote FTP server and return to user view.

Examples

Terminate the connection with the remote FTP server and return to user view.

```
[ftp] bye
221 Server closing.
```

cd

Syntax

cd { *directory* | **..** | **/** }

View

FTP client view

Default Level

3: Manage level

Parameters

directory: Name of the target directory, in the format of [*drive*:][*/*]*path*. *drive* represents the name of the storage medium, which is flash for the Switch 4210G. If *drive* is not specified, it indicates the file or subfolder under the current directory.

..: Returns to the upper directory, the function same as **cdup.**If the current working directory is the root directory, or there is no such an upper directory, the current working directory is not changed after the execution of the **cd** command. No command line help for this keyword.

/: Returns to the root directory of the storage medium. No command line help for this keyword.

Description

Use the **cd** command to change the current working directory on the remote FTP server.

You can use this command to access another authorized directory on the FTP server.

Related commands: **pwd**.

Examples

Change the working directory to the sub-directory **logfile** of the current directory.

```
[ftp] cd logfile
250 CWD command successful.
```

Change the working directory to the sub-directory **folder** of the authorized directory.

```
[ftp] cd /folder
250 CWD command successful.
```

cdup

Syntax

cdup

View

FTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **cdup** command to exit the current directory and enter the upper directory of the FTP server.

Execution of this command will not change the working directory if the current directory is already the authorized directory (that is, **work-directory**).

Related commands: **cd**, **pwd**.

Examples

Change the current working directory path to the upper directory.

```
[ftp] cdup
200 CDUP command successful.
```

close

Syntax

close

View

FTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **close** command to terminate the connection to the FTP server, but remain in FTP client view.

This command is equal to the **disconnect** command.

Examples

Terminate the connection to the FTP server and remain in FTP client view.

```
[ftp] close
221 Server closing.
[ftp]
```

debugging

Syntax

debugging

undo debugging

View

FTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **debugging** command to enable FTP client debugging.

Use the **undo debugging** command to disable FTP client debugging.

By default, FTP client debugging is disabled.

Examples

The device serves as the FTP client. Enable FTP client debugging and use the active mode to download file **sample.file** from the current directory of the FTP server.

```
<Sysname> terminal monitor
<Sysname> terminal debugging
<Sysname> ftp 192.168.1.46
Trying 192.168.1.46 ...
Press CTRL+K to abort
Connected to 192.168.1.46.
220 FTP service ready.
User(192.168.1.46:(none)):ftp
331 Password required for ftp.
Password:
230 User logged in.

[ftp]undo passive
[ftp] debugging
[ftp] get sample.file

---> PORT 192,168,1,44,4,21
200 Port command okay.
 The parsed reply is 200
---> RETR sample.file
150 Opening ASCII mode data connection for /sample.file.
 The parsed reply is 150
FTPC: File transfer started with the signal light turned on.
FTPC: File transfer completed with the signal light turned off.
```

```
.226 Transfer complete.
FTP: 3304 byte(s) received in 4.889 second(s), 675.00 byte(s)/sec.

[ftp]
```

Table 6-3 debugging command output description

Field	Description
---> PORT	Give an FTP order, with data port numbers being…
The parsed reply is	The received reply code, which is defined in RFC 959.
---> RETR	Download the file
FTPC: File transfer started with the signal light turned on.	File transfer starts, and the signal light is turned on.
FTPC: File transfer completed with the signal light turned off.	File transfer is completed, and the signal light is turned off.

delete

Syntax

delete *remotefile*

View

FTP client view

Default Level

3: Manage level

Parameters

remotefile: File name.

Description

Use the **delete** command to permanently delete a specified file on the remote FTP server.

To do this, you must be a user with the delete permission on the FTP server.

Examples

Delete file **temp.c**.

```
[ftp] delete temp.c
250 DELE command successful.
```

dir

Syntax

dir [*remotefile* [*localfile*]]

View

FTP client view

Default Level

3: Manage level

Parameters

remotefile: Name of the file or directory on the remote FTP server.

localfile: Name of the local file to save the displayed information.

Description

Use the **dir** command to view the detailed information of the files and subdirectories under the current directory on the remote FTP server.

Use the **dir** *remotefile* command to display the detailed information of the specified file or directory on the remote FTP server.

Use the **dir** *remotefile localfile* command to display the detailed information of the specified file or directory on the remote FTP server, and save the displayed information into a local file specified by the *localfile* argument.

Note

You can use the **dir** command to display the folder- and file-related information, such as the size, and the date they were created. If you only need to view the name of all the files and subdirectories under the current directory, you can use the **ls** command.

Examples

View the detailed information of the files and subdirectories under the current directory on the remote FTP server.

```
[ftp] dir
227 Entering Passive Mode (192,168,1,46,5,68).
125 ASCII mode data connection already open, transfer starting for /*.
drwxrwxrwx   1 noone    nogroup        0 Aug 08  2006 logfile
-rwxrwxrwx   1 noone    nogroup  20471748 May 11 10:21 test.bin
-rwxrwxrwx   1 noone    nogroup     4001 Dec 08  2007 config.cfg
-rwxrwxrwx   1 noone    nogroup     3608 Jun 13  2007 startup.cfg
drwxrwxrwx   1 noone    nogroup        0 Dec 03  2007 test
-rwxrwxrwx   1 noone    nogroup      299 Oct 15  2007 key.pub
226 Transfer complete.
FTP: 394 byte(s) received in 0.189 second(s), 2.00K byte(s)/sec.

[ftp]
```

View the information of the file **ar-router.cfg**, and save the result to **aa.txt**.

```
[ftp] dir ar-router.cfg aa.txt
```

```
227 Entering Passive Mode (192,168,1,50,17,158).
125 ASCII mode data connection already open, transfer starting for /ar-router.cfg.
....226 Transfer complete.
FTP: 67 byte(s) received in 4.600 second(s), 14.00 byte(s)/sec.
```

View the content of **aa.txt**.

```
[ftp] quit
<Sysname> more aa.txt
-rwxrwxrwx   1 noone    nogroup     3077 Jun 20 15:34 ar-router.cfg
```

disconnect

Syntax

disconnect

View

FTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **disconnect** command to disconnect from the remote FTP server but remain in FTP client view.

This command is equal to the **close** command.

Examples

Disconnect from the remote FTP server but remain in FTP client view.

```
[ftp] disconnect
221 Server closing.
```

display ftp client configuration

Syntax

display ftp client configuration

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ftp client configuration** command to display the configuration information of the FTP client.

Note

Currently this command displays the configured source IP address or source interface of the FTP client.

Related commands: **ftp client source**.

Examples

Display the current configuration information of the FTP client.

```
<Sysname> display ftp client configuration
The source IP address is 192.168.0.123
```

ftp

Syntax

ftp [*server-address* [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]]

View

User view

Default Level

3: Manage level

Parameters

server-address: IP address or host name (a string of 1 to 20 characters) of a remote FTP server.

service-port: TCP port number of the remote FTP server, in the range 0 to 65535. The default value is 21.

interface *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on this interface is the source address of the transmitted packets. If no primary IP address is configured on the source interface, the connection fails.

ip *source-ip-address:* The source IP address of the current FTP client. This source address must be the one that has been configured on the device.

Description

Use the **ftp** command to log in to the remote FTP server and enter FTP client view.

Note that:

- This command applies to IPv4 networks.
- If you use this command without specifying any parameters, you will simply enter the FTP client view without logging in to the FTP server.

- If you specify the parameters, you will be prompted to enter the username and password for accessing the FTP server.
- The priority of the source address specified with this command is higher than that with the **ftp client source** command. If you specify the source address with the **ftp client source** command first and then with the **ftp** command, the source address specified with the **ftp** command is used to communicate with the FTP server.

Related commands: **ftp client source**.

Examples

Log in from the current device **Sysname1** to the device **Sysname2** with the IP address of 192.168.0.211. The source IP address of the packets sent is 192.168.0.212.

```
<Sysname> ftp 192.168.0.211 source ip 192.168.0.212
Trying 192.168.0.211 ...
Press CTRL+K to abort
Connected to 192.168.0.211.
220 FTP Server ready.
User(192.168.0.211:(none)):abc
331 Password required for abc
Password:
230 User logged in.

[ftp]
```

ftp client source

Syntax

ftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo ftp client source

View

System view

Default Level

2: System level

Parameters

interface *interface-type interface-number*: Source interface for the FTP connection, including interface type and interface number. The primary IP address configured on the source interface is the source IP address of the packets sent by FTP. If no primary IP address is configured on the source interface, the connection fails.

ip *source-ip-address:* Source IP address of the FTP connection. It must be an IP address that has been configured on the device.

Description

Use the **ftp client source** command to configure the source address of the transmitted FTP packets from the FTP client.

Use the **undo ftp client source** command to restore the default.

By default, a device uses the IP address of the interface determined by the matched route as the source IP address to communicate with an FTP server.

Note that:

- The source address can be specified as the source interface and the source IP address. If you use the **ftp client source** command to specify the source interface and then the source IP address, the newly specified source IP address overwrites the configured source interface and vice versa.
- If the source address is specified with the **ftp client source** command and then with the **ftp** command, the source address specified with the latter one is used to communicate with the FTP server.
- The source address specified with the **ftp client source** command is valid for all FTP connections and the source address specified with the **ftp** command is valid only for the current FTP connection.

Related commands: **display ftp client configuration**.

Examples

Specify the source IP address of the FTP client as 2.2.2.2.

```
<Sysname> system-view
[Sysname] ftp client source ip 2.2.2.2
```

Specify the source interface of the FTP client as Vlan-interface 1.

```
<Sysname> system-view
[Sysname] ftp client source interface vlan-interface 1
```

ftp ipv6

Syntax

ftp ipv6 [*server-address* [*service-port*] [**source ipv6** *source-ipv6-address*] [**-i** *interface-type interface-number*]]

View

User view

Default Level

3: Manage level

Parameters

server-address: IP address or host name of the remote FTP server.

service-port: TCP port number of the FTP server, in the range 0 to 65535. The default value is 21.

source ipv6 *source-ipv6-address*: Specifies a source IPv6 address for transmitted FTP packets. This address must be an IPv6 address that has been configured on the device.

-i *interface-type interface-number*: Specifies the type and number of the egress interface. This parameter can be used only in case that the FTP server address is a link local address and the specified egress interface must have a link local address (For the configuration of link local addresses, see *IPv6 Basics* in the *IP Services Volume*).

Description

Use the **ftp ipv6** command to log in to the FTP server and enter FTP client view.

Note that:

- This command applies to IPv6 networks.
- If you use this command without specifying any parameters, you will simply enter the FTP client view without logging in to an FTP server.
- If you specify the parameters, you will be asked to enter the username and password for accessing the FTP server.

Examples

Log in to the FTP server with IPv6 address 3000::200.

```
<Sysname> ftp ipv6 3000::200
Trying 3000::200 ...
Press CTRL+K to abort
Connected to 3000::200.
220 Welcome!
User(3000::200:(none)): MY_NAME
331 Please specify the password.
Password:
230 Login successful.
[ftp]
```

get

Syntax

get *remotefile* [*localfile*]

View

FTP client view

Default Level

3: Manage level

Parameters

remotefile: Name of the file to be downloaded.

localfile: File name used after a file is downloaded and saved locally. If this argument is not specified, the file is saved locally using the source file name to the current working directory, namely the directory where the user executes the **ftp** command.

Description

Use the **get** command to download a file from a remote FTP server and save it.

Examples

Download file **testcfg.cfg** to the root directory of the storage medium of the master, and save it as **newest.cfg**.

```
[ftp] get startup.cfg newest.cfg

227 Entering Passive Mode (192,168,1,46,4,47).
125 ASCII mode data connection already open, transfer starting for /startup.cfg.
..226 Transfer complete.
FTP: 3608 byte(s) received in 2.050 second(s), 1.00K byte(s)/sec.
```

Download file **testcfg.cfg** to the root directory of the storage medium of the slave (with the member ID 2), and save it as **newest.cfg**.

```
[ftp] get startup.cfg slot2#flash:/newest.cfg

227 Entering Passive Mode (192,168,1,46,4,48).
125 ASCII mode data connection already open, transfer starting for /startup.cfg.
226 Transfer complete.
FTP: 3608 byte(s) received in 2.322 second(s), 1.00K byte(s)/sec.
```

lcd

Syntax

lcd

View

FTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **lcd** command to display the local working directory of the FTP client.

Examples

Display the local working directory.

```
[ftp] lcd
FTP: Local directory now flash:/clienttemp.
```

The above information indicates that the working directory of the FTP client before execution of the **ftp** command is **flash:/clienttemp**.

ls

Syntax

ls [*remotefile* [*localfile*]]

View

FTP client view

Default Level

3: Manage level

Parameters

remotefile: Filename or directory on the remote FTP server.

localfile: Name of a local file used to save the displayed information.

Description

Use the **ls** command to view the information of all the files and subdirectories under the current directory of the remote FTP server. The file names and subdirectory names are displayed.

Use the **ls** *remotefile* command to view the information of a specified file or subdirectory.

Use the **ls** *remotefile localfile* command to view the information of a specified file or subdirectory, and save the result to a local file specified by the *localfile* argument.

Note

The **ls** command can only display the names of files and directories on the FTP server, whereas the **dir** command can display other related information of the files and directories, such as the size, and the date they were created.

Examples

View the information of all files and subdirectories under the current directory of the FTP server.

```
[ftp] ls
227 Entering Passive Mode (192,168,1,50,17,165).
125 ASCII mode data connection already open, transfer starting for /*.
ar-router.cfg
logfile
mainar.bin
arbasicbtm.bin
ftp
test
bb.cfg
testcfg.cfg
226 Transfer complete.
FTP: 87 byte(s) received in 0.132 second(s) 659.00 byte(s)/sec.
```

View the information of directory **logfile**, and save the result to file **aa.txt**.

```
[ftp] ls logfile aa.txt
227 Entering Passive Mode (192,168,1,46,4,3).
125 ASCII mode data connection already open, transfer starting for /logfile/*.
....226 Transfer complete.
FTP: 20 byte(s) received in 3.962 second(s), 5.00 byte(s)/sec.
```

View the content of file **aa.txt**.

```
[ftp] quit
<Sysname> more aa.txt
.
..
logfile.log
```

mkdir

Syntax

mkdir *directory*

View

FTP client view

Default Level

3: Manage level

Parameters

directory: Name of the directory to be created.

Description

Use the **mkdir** command to create a subdirectory under the current directory on the remote FTP server.

To do this, you must be a user with the permission on the FTP server.

Examples

Create subdirectory **mytest** on the current directory of the remote FTP server.

```
[ftp] mkdir mytest
257 "/mytest" new directory created.
```

open

Syntax

open *server-address* [*service-port*]

View

FTP client view

Default Level

3: Manage level

Parameters

server-address: IP address or host name of a remote FTP server.

service-port: Port number of the remote FTP server, in the range 0 to 65535, with the default value of 21.

Description

Use the **open** command to log in to the IPv4 FTP server under FTP client view.

At login, you will be asked to enter the username and password for accessing the FTP server. If your input is correct, the login succeeds; otherwise, it fails.

If you have logged in to the IPv4 FTP server currently, you cannot use the **open** command to log in to another server. You need to disconnect with the current server first, and then try to connect with another one.

Related commands: **close**.

Examples

In FTP client view, log in to the FTP server with the IP address of 192.168.1.50.

```
<Sysname> ftp
[ftp] open 192.168.1.50
Trying 192.168.1.50 ...
Press CTRL+K to abort
Connected to 192.168.1.50.
220 FTP service ready.
User(192.168.1.50:(none)):aa
331 Password required for aa.
Password:
230 User logged in.

[ftp]
```

open ipv6

Syntax

open ipv6 *server-address* [*service-port*] [**-i** *interface-type interface-number*]

View

FTP client view

Default Level

3: Manage level

Parameters

server-address: IP address or host name of the remote FTP server.

service-port: Port number of the remote FTP server, in the range 0 to 65535. The default value is 21.

-i *interface-type interface-number*: Specifies the egress interface by its type and number. This parameter can be used only in case that the FTP server address is a link local address and the specified egress interface must have a link local address (For the configuration of link local addresses, see *IPv6 Basics* in the *IP Services Volume*).

Description

Use the **open ipv6** command to log in to the IPv6 FTP server in FTP client view.

At login, you will be asked to enter the username and password for accessing the FTP server. If your input is correct, the login succeeds; otherwise, it fails.

Related commands: **close**.

Examples

Log in to the FTP server (with IPv6 address 3000::200) in FTP client view.

```
<Sysname> ftp
[ftp] open ipv6 3000::200
Trying 3000::200 ...
Press CTRL+K to abort
Connected to 3000::200.
220 Welcome!
User(3000::200:(none)): MY_NAME
331 Please specify the password.
Password:
230 Login successful.
```

passive

Syntax

passive

undo passive

View

FTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **passive** command to set the data transmission mode to **passive**.

Use the **undo passive** command to set the data transmission mode to **active**.

The default transmission mode is **passive**.

Data transmission modes fall into the passive mode and the active mode. The active mode means that the data connection request is initiated by a server. The passive mode means that the data connection request is initiated by a client. This command is mainly used in conjunction with a firewall to restrict the FTP session connection between private and public network users.

Examples

Set the data transmission mode to **passive**.

```
[ftp] passive
FTP: passive is on
```

put

Syntax

put *localfile* [*remotefile*]

View

FTP client view

Default Level

3: Manage level

Parameters

localfile: Name of the local file to be uploaded.

remotefile: File name used after a file is uploaded and saved on the FTP server.

Description

Use the **put** command to upload a file on the client to the remote FTP server.

If no name is assigned to the file to be saved on the FTP server, the name of the source file is used by default. After a file is uploaded, it will be saved under the user's authorized directory, which can be set with the **authorization-attribute** command.

Examples

Upload source file **vrpcfg.cfg** on the master to the remote FTP server and save it as **ftpclient.cfg**.

```
[ftp] put vrpcfg.cfg ftpclient.cfg
227 Entering Passive Mode (192,168,1,46,4,50).
125 ASCII mode data connection already open, transfer starting for /ftpclient.cfg.
226 Transfer complete.
FTP: 1366 byte(s) sent in 0.064 second(s), 21.00Kbyte(s)/sec.
```

Upload source file **a.cfg** on the slave (with the member ID 2) to the remote FTP server and save it as **ftpclienta.cfg**.

```
[ftp] put slot2#flash:/a.cfg ftpclienta.cfg
227 Entering Passive Mode (192,168,1,46,4,52).
125 ASCII mode data connection already open, transfer starting for /ftpclienta.cfg.
226 Transfer complete.
FTP: 1226 byte(s) sent in 0.065 second(s), 18.00Kbyte(s)/sec.
```

pwd

Syntax

pwd

View

FTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **pwd** command to display the currently accessed directory on the remote FTP server.

Examples

Display the currently accessed directory on the remote FTP server.

```
[ftp] cd servertemp
[ftp] pwd
257 "/servertemp" is current directory.
```

The above information indicates that the **servertemp** folder under the root directory of the remote FTP server is being accessed by the user.

quit

Syntax

quit

View

FTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **quit** command to disconnect from the remote FTP server and exit to user view.

Examples

Disconnect from the remote FTP server and exit to user view.

```
[ftp] quit
221 Server closing.

<Sysname>
```

remotehelp

Syntax

remotehelp [*protocol-command*]

View

FTP client view

Default Level

3: Manage level

Parameters

protocol-command: FTP command.

Description

Use the **remotehelp** command to display the help information of FTP-related commands supported by the remote FTP server.

If no argument is specified, FTP-related commands supported by the remote FTP server are displayed.

Examples

Display FTP commands supported by the remote FTP server.

```
[ftp] remotehelp
214-Here is a list of available ftp commands
    Those with '*' are not yet implemented.
   USER   PASS   ACCT*  CWD    CDUP   SMNT*  QUIT   REIN*
   PORT   PASV   TYPE   STRU*  MODE*  RETR   STOR   STOU*
   APPE*  ALLO*  REST*  RNFR*  RNTO*  ABOR*  DELE   RMD
   MKD    PWD    LIST   NLST   SITE*  SYST   STAT*  HELP
   NOOP*  XCUP   XCWD   XMKD   XPWD   XRMD
214 Direct comments to 3COM company.
```

Display the help information for the **user** command.

```
[ftp] remotehelp user
214 Syntax: USER <sp> <username>.


[ftp]
```

Table 6-4 remotehelp command output description

Field	Description
214-Here is a list of available ftp commands	The following is an available FTP command list.
Those with '*' are not yet implemented.	Those commands with “*” are not yet implemented.
USER	Username
PASS	Password
CWD	Change the current working directory
CDUP	Change to parent directory
SMNT*	File structure setting
QUIT	Quit
REIN*	Re-initialization
PORT	Port number
PASV	Passive mode

Field	Description
TYPE	Request type
STRU*	File structure
MODE*	Transmission mode
RETR	Download a file
STOR	Upload a file
STOU*	Store unique
APPE*	Appended file
ALLO*	Allocation space
REST*	Restart
RNFR*	Rename the source
RNTO*	Rename the destination
ABOR*	Abort the transmission
DELE	Delete a file
RMD	Delete a folder
MKD	Create a folder
PWD	Print working directory
LIST	List files
NLST	List file description
SITE*	Locate a parameter
SYST	Display system parameters
STAT*	State
HELP	Help
NOOP*	No operation
XCUP	Extension command, the same meaning as CUP
XCWD	Extension command, the same meaning as CWD
XMKD	Extension command, the same meaning as MKD
XPWD	Extension command, the same meaning as PWD
XRMD	Extension command, the same meaning as RMD
Syntax: USER <sp> <username>.	Syntax of the **user** command: user (keyword) + space + *username*

rmdir

Syntax

rmdir *directory*

View

FTP client view

Default Level

3: Manage level

Parameters

directory: Directory name on the remote FTP server.

Description

Use the **rmdir** command to remove a specified directory from the FTP server.

Note that only authorized users are allowed to use this command.

Note that:

- The directory to be deleted must be empty, meaning you should delete all files and subdirectories under the directory before you delete a directory. For the deletion of files, refer to the **delete** command.
- After you execute the **rmdir** command successfully, the files in the remote recycle bin under the directory will be automatically deleted.

Examples

Delete the **temp1** directory from the authorized directory on the FTP server.

```
[ftp] rmdir /temp1
200 RMD command successful.
```

user

Syntax

user *username* [*password*]

View

FTP client view

Default Level

3: Manage level

Parameters

username: Login username.

password: Login password.

Description

Use the **user** command to relog in to the currently accessed FTP server with another username.

Before using this command, you must configure the corresponding username and password on the FTP server; otherwise, your login fails and the FTP connection is closed.

Examples

User **ftp1** has logged in to the FTP server. Use username **ftp2** to log in to the current FTP server. (Suppose username **ftp2** and password **123123123123** have been configured on the FTP server).

```
[ftp] user ftp2
331 Password required for ftp2.
Password:
230 User logged in.

[ftp]
```

verbose

Syntax

verbose

undo verbose

View

FTP client view

Default Level

3: Manage level

Parameters

None

Description

Use the **verbose** command to enable the protocol information function to display detailed prompt information.

Use the **undo verbose** command to disable the protocol information function.

By default, the protocol information function is enabled.

Examples

Enable the protocol information function.

```
[ftp] verbose
FTP: verbose is on
```

Disable the protocol information function and perform the Get operation.

```
[ftp] undo verbose
FTP: verbose is off

[ftp] get startup.cfg bb.cfg

FTP: 3608 byte(s) received in 0.052 second(s), 69.00K byte(s)/sec.
```

```
[ftp]
```

Enable the protocol information function and perform the Get operation.

```
[ftp] verbose
FTP: verbose is on

[ftp] get startup.cfg aa.cfg

227 Entering Passive Mode (192,168,1,46,5,85).
125 ASCII mode data connection already open, transfer starting for /startup.cfg.
226 Transfer complete.
FTP: 3608 byte(s) received in 0.193 second(s), 18.00K byte(s)/sec.
```

7 TFTP Configuration Commands

TFTP Client Configuration Commands

display tftp client configuration

Syntax

display tftp client configuration

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display tftp client configuration** command to display the configuration information of the TFTP client.

Related commands: **tftp client source**.

Examples

Display the current configuration information of the TFTP client.

```
<Sysname> display tftp client configuration
The source IP address is 192.168.0.123
```

Note

Currently this command displays the configured source IP address or source interface of the TFTP client.

tftp-server acl

Syntax

tftp-server [**ipv6**] **acl** *acl-number*

undo tftp-server [**ipv6**] **acl**

View

System view

Default Level

3: Manage level

Parameters

ipv6: References an IPv6 ACL. If it is not specified, an IPv4 ACL is referenced.

acl-number: Number of a basic ACL, in the range 2000 to 2999.

Description

Use the **tftp-server acl** command to control the access to the TFTP servers from the device through ACL.

Use the **undo tftp-server acl** command to restore the default.

By default, the access to the TFTP servers from the device is not controlled.

You can use the rules defined in the ACL to permit or deny the access from the device to the specified TFTP server on the network.

For more information about ACL, refer to *ACL Configuration* in the *Security Volume.*

Examples

In IPv4 networking environment, allow the device to access the TFTP server with the IP address of 1.1.1.1 only.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 1.1.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] tftp-server acl 2000
```

In IPv6 networking environment, allow the device to access the TFTP server with the IP address of 2001::1 only.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2001::1/128
[Sysname-acl6-basic-2001] quit
[Sysname] tftp-server ipv6 acl 2001
```

tftp

Syntax

tftp *server-address* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]

View

User view

Default Level

3: Manage level

Parameters

server-address: IP address or host name of a TFTP server.

get: Downloads a file in normal mode.

put: Uploads a file.

sget: Downloads a file in secure mode.

source-filename: Source file name.

destination-filename: Destination file name.

source: Configures parameters for source address binding.

- **interface** *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on the source interface is the source IP address of the packets sent by TFTP. If no primary IP address is configured on the source interface, the transmission fails.
- **ip** *source-ip-address:* Specifies the source IP address for the current TFTP client to transmit packets. This source address must be an IP address that has been configured on the device.

Description

Use the **tftp** command to upload files from the local device to a TFTP server or download files from the TFTP server to the local device.

- If no destination file name is specified, a file is saved using the same name as that on the remote TFTP server to the current working directory of the user (namely, the working directory where the **tftp** command is executed).
- The priority of the source address specified with this command is higher than that specified with the **tftp client source** command. If you use the **tftp client source** command to specify the source address first and then with the **tftp** command, the latter one is adopted.

This command applies to IPv4 networks.

Related commands: **tftp client source**.

Examples

Download the **config.cfg** file from the TFTP server with the IP address of 192.168.0.98 and save it as **config.bak**. Specify the source IP address to be 192.168.0.92.

```
<Sysname> tftp 192.168.0.98 get config.cfg config.bak source ip 192.168.0.92
  ...
  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait....
  TFTP:     372800 bytes received in 1 second(s)
  File downloaded successfully.
```

Upload the **config.cfg** file from the local device to the default path of the TFTP server with the IP address of 192.168.0.98 and save it as **config.bak**. Specify the source IP interface to be Vlan-interface 1.

```
<Sysname> tftp 192.168.0.98 put config.cfg config.bak source interface vlan-interface 1
```

```
  File will be transferred in binary mode
  Sending file to remote TFTP server. Please wait...
  TFTP:       345600 bytes sent in 1 second(s).
File uploaded successfully.
```

To upgrade the device, ddownload the **test.bin** file from the TFTP server with the IP address of 192.168.1.26 and save it to both the root directory on the flash of the master and the root directory on the flash of the slave (with the member ID 2).

```
<Sysname> tftp 192.168.1.26 get newest.bin startup.bin
  .
  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait..................
  TFTP:  2737556 bytes received in 13 second(s)
File downloaded successfully.
```

// Download the BIN file from the TFTP server to the root directory on the flash of the master.

```
<Sysname> tftp 192.168.1.26 get newest.bin slot2#flash:/startup.bin

  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait...|
  TFTP:  2737556 bytes received in 14 second(s)
File downloaded successfully.
```

// Download the BIN file from the TFTP server to the root directory on the flash of the slave.

tftp client source

Syntax

tftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo tftp client source

View

System view

Default Level

2: System level

Parameters

interface *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on the source interface is the source IP address of the packets sent by TFTP. If no primary IP address is configured on the source interface, the transmission fails.

ip *source-ip-address:* The source IP address of TFTP connections. It must be an IP address that has been configured on the device.

Description

Use the **tftp client source** command to configure the source address of the TFTP packets from the TFTP client.

Use the **undo telnet client source** command to restore the default.

By default, a device uses the IP address of the interface determined by the matched route as the source IP address to communicate with a TFTP server.

Note that:

- The source address can be specified as the source interface and the source IP; if you use the **tftp client source** command to specify the source interface and then the source IP, the newly specified source IP overwrites the configured source interface and vice versa.
- If the source address is specified with the **tftp client source** command and then with the **tftp** command, the source address specified with the latter one is used to communicate with the TFTP server.
- The source address specified with the **tftp client source** command is valid for all **tftp** connections and the source address specified with the **tftp** command is valid for the current **tftp** command.

Related commands: **display tftp client configuration**.

Examples

Specify the source IP address of the TFTP client as 2.2.2.2.

```
<Sysname> system-view
[Sysname] tftp client source ip 2.2.2.2
```

Specify the source interface of the TFTP client as Vlan-interface 1.

```
<Sysname> system-view
[Sysname] tftp client source interface vlan-interface 1
```

tftp ipv6

Syntax

tftp ipv6 *tftp-ipv6-server* [**-i** *interface-type interface-number*] { **get** | **put** } *source-file* [*destination-file*]

View

User view

Default Level

3: Manage level

Parameters

tftp-ipv6-server: IPv6 address or host name (a string of 1 to 46 characters) of a TFTP server.

-i *interface-type interface-number*: Specifies the egress interface by its type and number. This parameter can be used only in case that the TFTP server address is a link local address and the specified egress interface must have a link local address (For the configuration of link local address, see *IPv6 Basics* in the *IP Services Volume*).

get: Downloads a file.

put: Uploads a file.

source-filename: Source filename.

destination-filename: Destination filename. If not specified, this filename is the same as the source filename.

Description

Use the **tftp ipv6** command to download a specified file from a TFTP server or upload a specified local file to a TFTP server.

This command applies to IPv6 networks.

Examples

Download **filetoget.txt** from the TFTP server.

```
<Sysname> tftp ipv6 fe80::250:daff:fe91:e058 -i vlan-interface 1 get filetoget.txt
  ...
  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait....
  TFTP:     411100 bytes received in 2 second(s)
  File downloaded successfully.
```

8 HTTP Configuration Commands

HTTP Configuration Commands

display ip http

Syntax

display ip http

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ip http** command to display information about HTTP.

Examples

Display information about HTTP..

```
<Sysname> display ip http
HTTP port: 80
Basic ACL: 2222
Current connection: 0
Operation status: Running
```

Table 8-1 display ip http command output description

Field	Description
HTTP port	Port number used by the HTTP service
Basic ACL	A basic ACL number associated with the HTTP service
Current connection	The number of current connections
Operation status	Operation status, which takes the following values: • Running: The HTTP service is enabled. • Stopped: The HTTP service is disabled.

ip http acl

Syntax

ip http acl *acl-number*

undo ip http acl

View

System view

Default Level

2: System level

Parameters

acl-number: ACL number, in the range 2000 to 2999: basic IPv4 ACL

Description

Use the **ip http acl** command to associate the HTTP service with an ACL.

Use the **undo ip http acl** command to remove the association.

By default, the HTTP service is not associated with any ACL.

After the HTTP service is associated with an ACL, only the clients permitted by the ACL can access the device.

Related commands: **acl number** in *ACL Commands* in the *Security Volume.*

Examples

Configure to associate the HTTP service with ACL 2001 and only allow the clients within the 10.10.0.0/16 network segment to access the device through the Web function.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-basic-2001] quit
[Sysname] ip http acl 2001
```

ip http enable

Syntax

ip http enable

undo ip http enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **ip http enable** command to enable the HTTP service.

Use the **undo ip http enable** command to disable the HTTP service.

The device can act as the HTTP server and the users can access and control the device through the Web function only after the HTTP service is enabled.

Examples

Enable the HTTP service.

```
<Sysname> system-view
[Sysname] ip http enable
```

Disable the HTTP service.

```
<Sysname> system-view
[Sysname] undo ip http enable
```

ip http port

Syntax

ip http port *port-number*

undo ip http port

View

System view

Default Level

3: Manage level

Parameters

port-number: Port number of the HTTP service, in the range 1 to 65535.

Description

Use the **ip http port** command to configure the port number of the HTTP service.

Use the **undo ip http port** command to restore the default.

By default, the port number of the HTTP service is 80.

Note that this command does not check whether the configured port number conflicts with that of an existing service. Therefore, you must ensure that the port number is not used by another service before the configuration.

Examples

Configure the port number of the HTTP service as 8080.

```
<Sysname> system-view
[Sysname] ip http port 8080
```

9 HTTPS Configuration Commands

HTTPS Configuration Commands

display ip https

Syntax

display ip https

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ip https** command to display information about HTTPS.

Examples

Display information about HTTPS.

```
<Sysname> display ip https
HTTPS port: 443
SSL server policy: test
Certificate access-control-policy:
Basic ACL: 2222
Current connection: 0
Operation status: Running
```

Table 9-1 display ip https command output description

Field	Description
HTTPS port	Port number used by the HTTPS service
SSL server policy	The SSL server policy associated with the HTTPS service
Certificate access-control-policy	The certificate attribute access control policy associated with the HTTPS service
Basic ACL	The basic ACL number associated with the HTTPS service
Current connection	The number of current connections

Field	Description
Operation status	Operation status, which takes the following values: • Running: The HTTPS service is enabled. • Stopped: The HTTPS service is disabled.

ip https acl

Syntax

ip https acl *acl-number*

undo ip https acl

View

System view

Default Level

3: Manage level

Parameters

acl-number: ACL number, in the range 2000 to 2999: basic IPv4 ACL

Description

Use the **ip https acl** command to associate the HTTPS service with an ACL.

Use the **undo ip https acl** command to remove the association.

By default, the HTTPS service is not associated with any ACL.

After the HTTPS service is associated with an ACL, only the clients permitted by the ACL can access the device.

Related commands: **acl number** in *ACL Commands* in the *Security Volume*

Examples

Associate the HTTPS service with ACL 2001 and only allow the clients within the 10.10.0.0/16 network segment to access the HTTPS server through the Web function.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-basic-2001] quit
[Sysname] ip https acl 2001
```

ip https certificate access-control-policy

Syntax

ip https certificate access-control-policy *policy-name*

undo ip https certificate access-control-policy

View

System view

Default Level

3: Manage level

Parameters

policy-name: Name of the certificate attribute access control policy, a string of 1 to 16 characters.

Description

Use the **ip https certificate access-control-policy** command to associate the HTTPS service with a certificate attribute access control policy.

Use the **undo ip https certificate access-control-policy** command to remove the association.

By default, the HTTPS service is not associated with any certificate attribute access control policy.

Association of the HTTPS service with a certificate attribute access control policy can control the access rights of clients.

Related commands: **pki certificate access-control-policy**. (In *PKI Commands* in the *Security Volume*)

Examples

Associate the HTTPS server to certificate attribute access control policy **myacl**.

```
<Sysname> system-view
[Sysname] ip https certificate access-control-policy myacl
```

ip https enable

Syntax

ip https enable

undo ip https enable

View

System view

Default Level

3: Manage level

Parameters

None

Description

Use the ip https enable command to enable the HTTPS service.

Use the **undo ip https enable** command to disable the HTTPS service.

By default, the HTTPS service is disabled.

The device can act as the HTTP server and the users can access and control the device through the Web function only after the HTTP service is enabled.

Note that enabling of the HTTPS service triggers an SSL handshake negotiation process. During the process, if a local certificate of the device already exists, the SSL negotiation is successfully performed, and the HTTPS service can be started normally. If no local certificate exists, a certificate application process will be triggered by the SSL negotiation. Since the application process takes much time, the SSL negotiation often fails and the HTTPS service cannot be started normally. Therefore, the **ip https enable** command must be executed for multiple times to ensure normal startup of the HTTPS service.

Examples

Enable the HTTPS service.

```
<Sysname> system-view
[Sysname] ip https enable
```

ip https port

Syntax

ip https port *port-number*

undo ip https port

View

System view

Default Level

3: Manage level

Parameters

port-number: Port number of the HTTPS service, in the range 1 to 65535.

Description

Use the **ip https port** command to configure the port number of the HTTPS service.

Use the **undo ip https port** command to restore the default.

By default, the port number of the HTTPS service is 443.

Note that this command does not check whether the configured port number conflicts with that of an existing service. Therefore, you must ensure that the port number is not used by another service before the configuration.

Examples

Configure the port number of the HTTPS service as 6000.

```
<Sysname> system-view
[Sysname] ip https port 6000
```

ip https ssl-server-policy

Syntax

ip https ssl-server-policy *policy-name*

undo ip https ssl-server-policy

View

System view

Default Level

3: Manage level

Parameters

policy-name: Name of an SSL server policy, a string of 1 to 16 characters.

Description

Use the **ip https ssl-server-policy** command to associate the HTTPS service with an SSL server-end policy.

Use the **undo ip https ssl-server-policy** to remove the association between the HTTPS service and an SSL server-end policy.

By default, the HTTPS service is not associated with any SSL server-end policy.

Note that:

- The HTTPS service can be enabled only after this command is configured successfully.
- You cannot modify an SSL server-end policy or remove the association between the HTTPS service and an SSL server-end policy after the HTTS service is enabled.

Related commands: **ssl server-policy** in *SSL Commands* in the *Security Volume*

Examples

Configure the HTTPS service to use SSL server-end policy **myssl**.

```
<Sysname> system-view
[Sysname] ip https ssl-server-policy myssl
```

10 SNMP Configuration Commands

SNMP Configuration Commands

display snmp-agent community

Syntax

display snmp-agent community [read | write]

View

Any view

Default Level

1: Monitor level

Parameters

read: Displays the information of communities with read-only access right.

write: Displays the information of communities with read and write access right.

Description

Use the **display snmp-agent community** command to display community information for SNMPv1 or SNMPv2c.

Examples

Display the information of all the communities that have been configured.

```
<Sysname> display snmp-agent community
  Community name: aa
      Group name: aa
      Acl:2001
      Storage-type: nonVolatile

  Community name: bb
      Group name: bb
      Storage-type: nonVolatile

  Community name: userv1
      Group name: testv1
      Storage-type: nonVolatile
```

Table 10-1 display snmp-agent community command output description

Field	Description
Community name	Community name. • If a community name is created by using the **snmp-agent community** command, the community name will be displayed. • If a community name is created by using the **snmp-agent usm-user** { **v1** | **v2c** } command, the user name will be displayed.
Group name	SNMP group name. • If a community name is created by using the **snmp-agent community** command, the group name and the community name are the same, which means the community name will be displayed. • If a community name is created by using the **snmp-agent usm-user** { **v1** | **v2c** } command, the name of the group to which the user belongs will be displayed.
Acl	The number of the ACL in use. After an ACL is configured, only the Network Management Station (NMS) with the IP address that matches the ACL rule can access the device.
Storage-type	Storage type, which could be: • *volatile*: Information will be lost if the system is rebooted • *nonVolatile*: Information will not be lost if the system is rebooted • *permanent*: Information will not be lost if the system is rebooted. Modification is permitted, but deletion is forbidden • *readOnly*: Information will not be lost if the system is rebooted. Read only, that is, no modification, no deletion • *other*: Other storage types

display snmp-agent group

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

group-name: Specifies the SNMP group name, a string of 1 to 32 characters, case sensitive.

Description

Use the **display snmp-agent group** command to display information for the SNMP agent group, including group name, security model, MIB view, storage type, and so on. Absence of the *group-name* parameter indicates that information for all groups will be displayed.

Examples

Display the information of all SNMP agent groups.

```
<Sysname> display snmp-agent group
  Group name: groupv3
      Security model: v3 noAuthnoPriv
      Readview: ViewDefault
      Writeview: <no specified>
      Notifyview: <no specified>
      Storage-type: nonVolatile
```

Table 10-2 display snmp-agent group command output description

Field	Description
Group name	SNMP group name
Security model	Security model of the SNMP group, which can be: authPriv (authentication with privacy), authNoPriv (authentication without privacy), or noAuthNoPriv (no authentication no privacy).
Readview	The read only MIB view associated with the SNMP group
Writeview	The writable MIB view associated with the SNMP group
Notifyview	The notify MIB view associated with the SNMP group, the view with entries that can generate traps
Storage-type	Storage type, which includes: volatile, nonVolatile, permanent, readOnly, and other. For detailed information, refer to Table 10-1.

display snmp-agent local-engineid

Syntax

display snmp-agent local-engineid

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display snmp-agent local-engineid** command to display the local SNMP agent engine ID.

SNMP engine ID identifies an SNMP entity uniquely within an SNMP domain. SNMP engine is an indispensable part of an SNMP entity. It provides the SNMP message allocation, message handling, authentication, and access control.

Examples

Display the local SNMP agent engine ID.

```
<Sysname> display snmp-agent local-engineid
SNMP local EngineID: 800007DB7F0000013859
```

display snmp-agent mib-view

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

exclude: Displays MIB view information of the **excluded** type.

include: Displays MIB view information of the **included** type.

viewname *view-name*: Displays MIB view information with a specified MIB view name, where *view-name* is the name of the specified MIB view.

Description

Use the **display snmp-agent mib-view** command to display MIB view information. Absence of parameters indicates that information for all MIB views will be displayed.

Examples

Display all SNMP MIB views of the device.

```
<Sysname> display snmp-agent mib-view
  View name:ViewDefault
     MIB Subtree:iso
     Subtree mask:
     Storage-type: nonVolatile
     View Type:included
     View status:active

  View name:ViewDefault
     MIB Subtree:snmpUsmMIB
     Subtree mask:
     Storage-type: nonVolatile
     View Type:excluded
     View status:active

  View name:ViewDefault
     MIB Subtree:snmpVacmMIB
     Subtree mask:
     Storage-type: nonVolatile
     View Type:excluded
     View status:active

  View name:ViewDefault
     MIB Subtree:snmpModules.18
```

```
Subtree mask:
Storage-type: nonVolatile
View Type:excluded
View status:active
```

ViewDefault is the default view of the device. When you access the device through the ViewDefault view, you can access all the MIB objects of the iso subtree except for the MIB objects under the snmpUsmMIB, snmpVacmMIB, and snmpModules.18 subtrees.

Table 10-3 display snmp-agent mib-view command output description

Field	Description
View name	MIB view name
MIB Subtree	MIB subtree corresponding to the MIB view
Subtree mask	MIB subtree mask
Storage-type	Storage type
View Type	View type, which can be **included** or **excluded**: • Included indicates that all nodes of the MIB tree are included in current view, namely, you are allowed to access all the MIB objects of the subtree • Excluded indicates that none of the nodes of the MIB tree are included in current view, namely, you are allowed to access none of the MIB objects of the subtree
View status	The status of MIB view

display snmp-agent statistics

Syntax

display snmp-agent statistics

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display snmp-agent statistics** command to display SNMP statistics.

Examples

Display the statistics on the current SNMP.

```
<Sysname> display snmp-agent statistics
  1684 Messages delivered to the SNMP entity
  5 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
1679 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 (Maximum packet size 1500)
16544 MIB objects retrieved successfully
2 MIB objects altered successfully
7 GetRequest-PDU accepted and processed
7 GetNextRequest-PDU accepted and processed
1653 GetBulkRequest-PDU accepted and processed
1669 GetResponse-PDU accepted and processed
2 SetRequest-PDU accepted and processed
0 Trap PDUs accepted and processed
0 Alternate Response Class PDUs dropped silently
0 Forwarded Confirmed Class PDUs dropped silently
```

Table 10-4 display snmp-agent statistics command output description

Field	Description
Messages delivered to the SNMP entity	Number of packets delivered to the SNMP agent
Messages which were for an unsupported version	Number of packets from a device with an SNMP version that is not supported by the current SNMP agent
Messages which used a SNMP community name not known	Number of packets that use an unknown community name
Messages which represented an illegal operation for the community supplied	Number of packets carrying an operation that the community has no right to perform
ASN.1 or BER errors in the process of decoding	Number of packets with ASN.1 or BER errors in the process of decoding
Messages passed from the SNMP entity	Number of packets sent by the SNMP agent
SNMP PDUs which had badValue error-status	Number of SNMP PDUs with a badValue error
SNMP PDUs which had genErr error-status	Number of SNMP PDUs with a genErr error
SNMP PDUs which had noSuchName error-status	Number of PDUs with a noSuchName error
SNMP PDUs which had tooBig error-status (Maximum packet size 1500)	Number of PDUs with a tooBig error (the maximum packet size is 1,500 bytes)
MIB objects retrieved successfully	Number of MIB objects that have been successfully retrieved
MIB objects altered successfully	Number of MIB objects that have been successfully modified
GetRequest-PDU accepted and processed	Number of get requests that have been received and processed
GetNextRequest-PDU accepted and processed	Number of getNext requests that have been received and processed
GetBulkRequest-PDU accepted and processed	Number of getBulk requests that have been received and processed

Field	Description
GetResponse-PDU accepted and processed	Number of get responses that have been received and processed
SetRequest-PDU accepted and processed	Number of set requests that have been received and processed
Trap PDUs accepted and processed	Number of traps that have been received and processed
Alternate Response Class PDUs dropped silently	Number of dropped response packets
Forwarded Confirmed Class PDUs dropped silently	Number of forwarded packets that have been dropped

display snmp-agent sys-info

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

contact: Displays the contact information of the current network administrator.

location: Displays the location information of the current device.

version: Displays the version of the current SNMP agent.

Description

Use the **display snmp-agent sys-info** command to display the current SNMP system information.

If no keyword is specified, all SNMP agent system information will be displayed.

Examples

Display the current SNMP agent system information.

```
<Sysname> display snmp-agent sys-info
  The contact person for this managed node:
        3Com Corporation.

  The physical location of this node:
        Marlborough, MA 01752 USA

  SNMP version running in the system:
        SNMPv3
```

display snmp-agent trap queue

Syntax

display snmp-agent trap queue

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display snmp-agent trap queue** command to display basic information of the trap queue, including trap queue name, queue length and the number of traps in the queue currently.

Related commands: **snmp-agent trap life**, **snmp-agent trap queue-size**.

Examples

Display the current configuration and usage of the trap queue.

```
<Sysname> display snmp-agent trap queue
  Queue name: SNTP
  Queue size: 100
  Message number: 6
```

Table 10-5 display snmp-agent trap queue command output description

Field	Description
Queue name	Trap queue name
Queue size	Trap queue size
Message number	Number of traps in the current trap queue

display snmp-agent trap-list

Syntax

display snmp-agent trap-list

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display snmp-agent trap-list** command to display the modules that can generate traps and whether their trap function is enabled or not. If a module comprises multiple sub-modules, then as long as one sub-module has the trap function enabled, the whole module will be displayed as being enabled with the trap function.

Related commands: **snmp-agent trap enable**.

Examples

Display the modules that can generate traps and whether their trap function is enabled or not.

```
<Sysname> display snmp-agent trap-list
  configuration trap enable
  flash trap enable
  standard trap enable
  system trap enable

  Enable traps: 4; Disable traps: 0
```

In the above output, enable indicates that the module is allowed to generate traps whereas disable indicates the module is not allowed to generate traps. You can configure the trap function (enable or disable) of each module through command lines.

display snmp-agent usm-user

Syntax

display snmp-agent usm-user [engineid *engineid* | username *user-name* | group *group-name*] *

View

Any view

Default Level

1: Monitor level

Parameters

engineid *engineid*: Displays SNMPv3 user information for a specified engine ID, where *engineid* indicates the SNMP engine ID.

username *user-name*: Displays SNMPv3 user information for a specified user name. It is case sensitive.

group *group-name*: Displays SNMPv3 user information for a specified SNMP group name. It is case sensitive.

Description

Use the **display snmp-agent usm-user** command to display SNMPv3 user information.

Examples

Display SNMPv3 information of all created users.

```
<Sysname> display snmp-agent usm-user
  User name: userv3
```

```
Group name: mygroupv3
    Engine ID: 800063A203000FE240A1A6
    Storage-type: nonVolatile
    UserStatus: active

User name: userv3code
Group name: groupv3code
    Engine ID: 800063A203000FE240A1A6
    Storage-type: nonVolatile
    UserStatus: active
```

Table 10-6 display snmp-agent usm-user command output description

Field	Description
User name	SNMP user name
Group name	SNMP group name
Engine ID	Engine ID for an SNMP entity
Storage-type	Storage type, which can be the following: • volatile • nonvolatile • permanent • readOnly • other See Table 10-1 for details.
UserStatus	SNMP user status

enable snmp trap updown

Syntax

enable snmp trap updown

undo enable snmp trap updown

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **enable snmp trap updown** command to enable the trap function for interface state changes.

Use the **undo enable snmp trap updown** command to disable the trap function for interface state changes.

By default, the trap function for interface state changes is enabled.

Note that:

To enable an interface to generate linkUp/linkDown traps when its state changes, you need to enable the linkUp/linkDown trap function on the interface and globally. Use the **enable snmp trap updown** command to enable this function on an interface, and use the **snmp-agent trap enable** [**standard** [**linkdown** | **linkup**] *] command to enable this function globally.

Related commands: **snmp-agent target-host**, **snmp-agent trap enable**.

Examples

Enable the sending of linkUp/linkDown SNMP traps on port GigabitEthernet 1/0/1 and use the community name **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] enable snmp trap updown
```

snmp-agent

Syntax

snmp-agent

undo snmp-agent

View

System view

Default Level

3: Manage level

Parameters

None

Description

Use the **snmp-agent** command to enable SNMP agent.

Use the **undo snmp-agent** command to disable SNMP agent.

By default, SNMP agent is disabled.

You can enable SNMP agent through any commands that begin with **snmp-agent**.

Examples

Enable SNMP agent on the device.

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

snmp-agent calculate-password

Syntax

snmp-agent calculate-password *plain-password* **mode** { **3desmd5** | **3dessha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

View

System view

Default Level

3: Manage level

Parameters

plain-password: Plain text password to be encrypted, a string of 1 to 64 characters.

mode: Specifies the encryption algorithm and authentication algorithm. The three encryption algorithms Advanced Encryption Standard (AES), triple data encryption standard (3DES), and Data Encryption Standard (DES) are in descending order in terms of security. Higher security means more complex implementation mechanism and lower speed. DES is enough to meet general requirements. Message-Digest Algorithm 5 (MD5) and Secure Hash Algorithm (SHA-1) are the two authentication algorithms. MD5 is faster than SHA-1, while SHA-1 provides higher security than MD5.

- **3desmd5**: Converts a plain text encryption password to a cipher text encryption password. In this case, the authentication protocol must be MD5, and the encryption algorithm must be 3DES.
- **3dessha**: Converts a plain text encryption password to a cipher text encryption password. In this case, the authentication protocol must be SHA-1, and the encryption algorithm must be 3DES.
- **md5**: Converts a plain text authentication password to a cipher text authentication password. In this case, the authentication protocol must be MD5. Or, this algorithm can convert the plain text encryption password to a cipher text encryption password, In this case, the authentication protocol must be MD5, and the encryption algorithm can be either AES or DES (when the authentication protocol is specified as MD5, cipher text passwords are the same by using the encryption algorithms AES and DES).
- **sha**: Converts the plain text authentication password to a cipher text authentication password. In this case, the authentication protocol must be SHA-1. Or, this algorithm can convert the plain text encryption password to a cipher text encryption password, In this case, the authentication protocol must be SHA-1, and the encryption algorithm can be either AES or DES (when the authentication protocol is specified as SHA-1, cipher text passwords are the same by using the encryption algorithms AES and DES).

local-engineid: Uses local engine ID to calculate cipher text password. For engine ID-related configuration, refer to the **snmp-agent local-engineid** command.

specified-engineid: Uses user-defined engine ID to calculate cipher text password.

engineid: The engine ID string, an even number of hexadecimal characters, in the range 10 to 64. Its length must not be an odd number, and the all-zero and all-F strings are invalid.

Description

Use the **snmp-agent calculate-password** command to convert the user-defined plain text password to a cipher text password.

Note that:

- The cipher text password converted with the **sha** keyword specified in this command is a string of 40 hexadecimal characters. For an authentication password, all of the 40 hexadecimal characters are valid; while for a privacy password, only the first 32 hexadecimal characters are valid.
- Enable SNMP on the device before executing the command.

When creating an SNMPv3 user, if you specify to use the cipher text authentication/encryption password, you can use this command to generate a cipher text password.

The converted password is associated with the engine ID, namely, the password is valid only under the specified engine ID based on which the password was configured.

Related commands: snmp-agent usm-user v3.

Examples

Use local engine ID and MD5 authentication protocol to convert the plain text password **authkey**.

```
<Sysname> system-view
[Sysname] snmp-agent calculate-password authkey mode md5 local-engineid
The secret key is: 09659EC5A9AE91BA189E5845E1DDE0CC
```

snmp-agent community

Syntax

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

undo snmp-agent community { **read** | **write** } *community-name*

View

System view

Default Level

3: Manage level

Parameters

read: Indicates that the community has read only access right to the MIB objects; that is, the NMS can perform read-only operations when it uses this community name to access the agent.

write: Indicates that the community has read and write access right to the MIB objects; that is, the NMS can perform read and write operations when it uses this community name to access the agent.

community-name: Community name, a string of 1 to 32 characters.

acl *acl-number*: Associates a basic ACL with the community name. *acl-number* is in the range 2,000 to 2,999. By using an ACL, you can configure to allow or prohibit the access to the agent from the NMS with the specified source IP address.

mib-view *view-name*: Specifies the MIB view name associated with *community-name*, where *view-name* represents the MIB view name, a string of 1 to 32 characters. If no keyword is specified, the default view is ViewDefault (The view created by the system after SNMP agent is enabled).

Description

Use the **snmp-agent community** command to create a new SNMP community. Parameters to be configured include access right, community name, ACL, and accessible MIB views.

Use the **undo snmp-agent community** command to delete a specified community.

The community name configured with this command is only valid for the SNMP v1 and v2c agent.

A community is composed of NMSs and SNMP agents, and is identified by the community name, which functions as a password. In a community, when devices communicate with each other, they use community name for authentication. The NMS and the SNMP agent can access each other only when they are configured with the same community name. Typically, **public** is used as the read-only community name, and **private** is used as the read and write community name. For security purposes, you are recommended to configure a community name other than **public** and **private**.

- The keyword **acl** specifies that only the NMS with a qualified IP address can access the agent.
- The argument *community-name* specifies the community name used by the NMS when it accesses the agent.
- The keyword **mib-view** specifies the MIB objects which the NMS can access.
- The keywords **read** and **write** specify the access type.

Related commands: **snmp-agent mib-view**.

Examples

Create a community with the name of **readaccess**, allowing read-only access right using this community name.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] snmp-agent community read readaccess
```

- Set the SNMP version on the NMS to SNMPv1 or SNMPv2c
- Fill in the read-only community name **readaccess**
- Establish a connection, and the NMS can perform read-only operations to the MIB objects in the ViewDefault view on the device

Create a community with the name of **writeaccess**, allowing only the NMS with the IP address of 1.1.1.1 to configure the values of the agent MIB objects by using this community name; other NMSs are not allowed to perform the write operations by using this community name.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-basic-2001] rule deny source any
[Sysname-acl-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community write writeaccess acl 2001
```

- Set the IP address of the NMS to 1.1.1.1
- Set the SNMP version on the NMS to SNMPv2c
- Fill in the write community name **writeaccess**; namely, the NMS can perform read-only operations to the MIB objects in the ViewDefault view on the device

Create a community with the name of **wr-sys-acc**. The NMS can perform the read and write operations to the MIB objects of the system subtree (with the OID of 1.3.6.1.2.1.1).

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v1 v2c
[Sysname] snmp-agent mib-view included test system
[Sysname] snmp-agent community write wr-sys-acc mib-view system
```

- Set the SNMP version on the NMS to SNMPv1 or SNMPv2c
- Fill in the write community name **wr-sys-acc**

- Establish a connection, and the NMS can perform read and write operations to the MIB objects in system view on the device

snmp-agent group

Syntax

The following syntax applies to SNMPv1 and SNMP v2c:

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]

undo snmp-agent group { **v1** | **v2c** } *group-name*

The following syntax applies to SNMPv3:

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

undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

View

System view

Default Level

3: Manage level

Parameters

v1: SNMPv1.

v2c: SNMPv2c.

v3: SNMPv3.

group-name: Group name, a string of 1 to 32 characters.

authentication: Specifies the security model of the SNMP group to be authentication only (without privacy).

privacy: Specifies the security model of the SNMP group to be authentication and privacy.

read-view *read-view*: Read view, a string of 1 to 32 characters. The default read view is ViewDefault.

write-view *write-view:* Write view, a string of 1 to 32 characters. By default, no write view is configured, namely, the NMS cannot perform the write operations to all MIB objects on the device.

notify-view *notify-view*: Notify view, for sending traps, a string of 1 to 32 characters. By default, no notify view is configured, namely, the agent does not send traps to the NMS.

acl *acl-number*: Associates a basic ACL with the group. *acl-number* is in the range 2000 to 2999. By using a basic ACL, you can restrict the source IP address of SNMP packets, that is, you can configure to allow or prohibit SNMP packets with a specific source IP address, so as to restrict the intercommunication between the NMS and the agent.

Description

Use the **snmp-agent group** command to configure a new SNMP group and specify its access right.

Use the **undo snmp-agent group** command to delete a specified SNMP group.

By default, SNMP groups configured by the **snmp-agent group v3** command use a no-authentication-no-privacy security model.

An SNMP group defines security model, access right, and so on. A user in this SNMP group has all these public properties.

Related commands: **snmp-agent mib-view**, **snmp-agent usm-user**.

Examples

Create an SNMP group **group1** on an SNMPv3 enabled device, no authentication, no privacy.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 group1
```

snmp-agent local-engineid

Syntax

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

View

System view

Default Level

3: Manage level

Parameters

engineid: Engine ID, an even number of hexadecimal characters, in the range 10 to 64. Its length must not be an odd number, and the all-zero and all-F strings are invalid.

Description

Use the **snmp-agent local-engineid** command to configure a local engine ID for an SNMP entity.

Use the **undo snmp-agent local-engineid** command to restore the default local engine ID.

By default, the engine ID of a device is the combination of company ID and device ID. Device ID varies by product; it could be an IP address, a MAC address, or a self-defined string of hexadecimal numbers.

An engine ID has two functions:

- For all devices managed by one NMS, each device needs a unique engine ID to identify the SNMP agent. By default, each device has an engine ID. The network administrator has to ensure that there is no repeated engine ID within an SNMP domain.
- In SNMPv3, the user name and cipher text password are associated with the engine ID. Therefore, if the engine ID changes, the user name and cipher text password configured under the engine ID become invalid.

Typically, the device uses its default engine ID. For ease of remembrance, you can set engine IDs for the devices according to the network planning. For example, if both device 1 and device 2 are on the first floor of building A, you can set the engine ID of device 1 to 000Af0010001, and that of device 2 to 000Af0010002.

Related commands: **snmp-agent usm-user**.

Examples

Configure the local engine ID as **123456789A**.

```
<Sysname> system-view
[Sysname] snmp-agent local-engineid 123456789A
```

snmp-agent log

Syntax

snmp-agent log { **all** | **get-operation** | **set-operation** }

undo snmp-agent log { **all** | **get-operation** | **set-operation** }

View

System view

Default Level

3: Manage level

Parameters

all: Enables logging of SNMP GET and SET operations.

get-operation: Enables logging of SNMP GET operation.

set-operation: Enables logging of SNMP SET operation.

Description

Use the **snmp-agent log** command to enable SNMP logging.

Use the **undo snmp-agent log** command to restore the default.

By default, SNMP logging is disabled.

If specified SNMP logging is enabled, when the NMS performs a specified operation to the SNMP agent, the latter records the operation-related information and saves it to the information center. With parameters for the information center set, output rules of the SNMP logs are decided (that is, whether logs are permitted to output and the output destinations).

Examples

Enable logging of SNMP GET operation.

```
<Sysname> system-view
[Sysname] snmp-agent log get-operation
```

Enable logging of SNMP SET operation.

```
<Sysname> system-view
[Sysname] snmp-agent log set-operation
```

snmp-agent mib-view

Syntax

snmp-agent mib-view { excluded | included } *view-name oid-tree* [mask *mask-value*]

undo snmp-agent mib-view *view-name*

View

System view

Default Level

3: Manage level

Parameters

excluded: Indicates that no nodes of the MIB tree are included in current view.

included: Indicates that all nodes of the MIB tree are included in current view.

view-name: View name, a string of 1 to 32 characters.

oid-tree: MIB subtree, identified by the OID of the subtree root node, such as 1.4.5.3.1, or the name of the subtree root node, such as “system”. OID is made up of a series of integers, which marks the position of the node in the MIB tree and uniquely identifies a MIB object.

mask *mask-value*: Mask for a MIB subtree, in the range 1 to 32 hexadecimal digits. It must be an even digit.

Description

Use the **snmp-agent mib-view** command to create or update MIB view information so that MIB objects can be specified.

Use the **undo snmp-agent mib-view** command to delete the current configuration.

By default, MIB view name is ViewDefault.

MIB view is a subset of MIB, and it may include all nodes of a MIB subtree (that is, the access to all nodes of this MIB subtree is permitted), or may exclude all nodes of a MIB subtree (that is, the access to all nodes of this MIB subtree is forbidden).

You can use the **display snmp-agent mib-view** command to view the access right of the default view. Also, you can use the **undo snmp-agent mib-view** command to remove the default view, after that, however, you may not be able to read or write all MIB nodes on the agent.

Related commands: **snmp-agent group**.

Examples

Create a MIB view **mibtest**, which includes all objects of the subtree **mib-2**, and excludes all objects of the subtree **ip**.

```
<Sysname> system-view
[Sysname] snmp-agent mib-view included mibtest 1.3.6.1
[Sysname] snmp-agent mib-view excluded mibtest ip
[Sysname] snmp-agent community read public mib-view mibtest
```

If the SNMP version on the NMS is set to SNMPv1, when the NMS uses the community name **public** to access the device, it cannot access all objects of the **ip** subtree (such as the ipForwarding node, the ipDefaultTTL node, and so on), but it can access all objects of the **mib-2** subtree.

snmp-agent packet max-size

Syntax

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

undo snmp-agent packet max-size

View

System view

Default Level

3: Manage level

Parameters

byte-count: Maximum size of the SNMP packets that can be received or sent by the agent, in the range 484 to 17,940.

Description

Use the **snmp-agent packet max-size** command to configure the maximum size of the SNMP packets that can be received or sent by the agent.

Use the **undo snmp-agent packet max-size** command to restore the default packet size.

By default, the maximum size of the SNMP packets that can be received or sent by the agent is 1,500 bytes.

If devices not supporting fragmentation exist on the routing path between the NMS and the agent, you can use the command to configure the maximum SNMP packet size, and thus to prevent giant packets from being discarded.

Typically, you are recommended to apply the default value.

Examples

Configure the maximum size of the SNMP packets that can be received or sent by the SNMP agent as 1,042 bytes.

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

snmp-agent sys-info

Syntax

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

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

View

System view

Default Level

3: Manage level

Parameters

contact *sys-contact*: A string of 1 to 200 characters that describes the contact information for system maintenance.

location *sys-location*: A string of 1 to 200 characters that describes the location of the device.

version: The SNMP version in use.

- **all**: Specifies SNMPv1, SNMPv2c, and SNMPv3.
- **v1**: SNMPv1.
- **v2c**: SNMPv2c.
- **v3**: SNMPv3.

Description

Use the **snmp-agent sys-info** command to configure system information, including the contact information, the location, and the SNMP version in use.

Use the **undo snmp-agent sys-info contact** and **undo snmp-agent sys-info location** command to restore the default.

Use the **undo snmp-agent sys-info version** command to disable use of the SNMP function of the specified version.

By default, the location information is Marlborough, MA 01752 USA, version is SNMPv3, and the contact is 3Com Corporation.

The device can process the SNMP packets of the corresponding version only if SNMP of a specific version is enabled. If SNMPv1 is enabled, the device will drop the received SNMPv2c packets; if SNMPv2c is enabled, the device will drop the received SNMPv1 packets. To enable the device to communicate with different NMSs, you can enable SNMP of different versions on a device.

Related commands: **display snmp-agent sys-info**.

Note

Network maintenance engineers can use the system contact information to get in touch with the manufacturer in case of network failures. The system location information is a management variable under the system branch as defined in RFC1213-MIB, identifying the location of the managed object.

Examples

Configure the contact information as “Dial System Operator at beeper # 27345”.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info contact Dial System Operator at beeper # 27345
```

snmp-agent target-host

Syntax

snmp-agent target-host trap address udp-domain { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host trap address udp-domain { *ip-address* | **ipv6** *ipv6-address* } **params securityname** *security-string*

View

System view

Default Level

3: Manage level

Parameters

trap: Specifies the host to be the target host which will receive traps and notifications from the device.

address: Specifies the destination IP address in the SNMP messages sent from the device.

udp-domain: Indicates that the trap is transmitted using UDP.

ip-address: The IPv4 address of the trap target host.

ipv6 *ipv6-address*: Specifies the IPv6 address of the trap target host.

udp-port *port-number*: Specifies the number of the port on the target host to receive traps.

params securityname *security-string*: Specifies the authentication related parameter, which is an SNMPv1 or SNMPv2c community name or an SNMPv3 user name, a string of 1 to 32 characters.

v1: SNMPv1.

v2c: SNMPv2c.

v3: SNMPv3.

- **authentication**: Specifies the security model to be authentication without privacy. Authentication is a process to check whether the packet is integral and whether it has been tampered. You need to configure the authentication password when creating an SNMPv3 user.
- **privacy**: Specifies the security model to be authentication with privacy. Privacy is to encrypt the data part of a packet to prevent it from being intercepted. You need to configure the authentication password and privacy password when creating an SNMPv3 user.

Description

Use the **snmp-agent target-host** command to configure the related settings for a trap target host.

Use the **undo snmp-agent target-host** command to remove the current settings. According to the networking requirements, you can use this command for multiple times to configure different settings for a target host, enabling the device to send trap messages to different NMSs.

- If **udp-port** *port-number* is not specified, port number 162 is used.
- If the key words **v1, v2** and **v3** are not specified, v1 is used.
- If the key words **authentication** and **privacy** are not specified, the authentication mode is no authentication, no privacy.

Related commands: **enable snmp trap updown**, **snmp-agent trap enable**, **snmp-agent trap source**, **snmp-agent trap life**.

Examples

Enable the device to send SNMP traps to 10.1.1.1, using the community name of **public**.

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

snmp-agent trap enable

Syntax

snmp-agent trap enable [**configuration** | **flash** | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system**]

undo snmp-agent trap enable [**configuration** | **flash** | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system**]

View

System view

Default Level

3: Manage level

Parameters

configuration: Enables the sending of configuration traps.

flash: Enables the sending of FLASH-related traps.

standard: Standard traps.

- **authentication**: Enables the sending of authentication failure traps in the event of authentication failure.
- **coldstart**: Sends coldstart traps when the device restarts.
- **linkdown**: Sends linkdown traps when the port is in a linkdown status. It should be configured globally.
- **linkup**: Sends linkup traps when the port is in a linkup status. It should be configured globally.
- **warmstart**: Sends warmstart traps when the SNMP restarts.

system: Sends 3Com-SYS-MAN-MIB (a private MIB) traps.

Description

Use the **snmp-agent trap enable** command to enable the trap function globally.

Use the **undo snmp-agent trap enable** command to disable the trap function globally.

By default, the trap function of other modules is enabled.

Only after the trap function is enabled can each module generate corresponding traps.

Note that:

To enable an interface to generate Linkup/Linkdown traps when its state changes, you need to enable the linkUp/linkDown trap function on the interface and globally. Use the **enable snmp trap updown** command to enable this function on an interface, and use the **snmp-agent trap enable** [**standard** [**linkdown** | **linkup**] *] command to enable this function globally.

Related commands: **snmp-agent target-host**, **enable snmp trap updown**.

Examples

Enable the device to send SNMP authentication failure packets to 10.1.1.1, using the community name **public**.

```
<Sysname> system-view
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public
```

```
[Sysname] snmp-agent trap enable standard authentication
```

snmp-agent trap if-mib link extended

Syntax

snmp-agent trap if-mib link extended

undo snmp-agent trap if-mib link extended

View

System view

Default Level

3: Manage level

Parameters

None

Description

Use the **snmp-agent trap if-mib link extended** command to extend the standard linkUp/linkDown traps defined in RFC. An extended linkUp/linkDown trap is the standard linkUp/linkDown trap defined in RFC appended with the interface description and interface type information.

Use the **undo snmp-agent trap if-mib link extended** command to restore the default.

By default, standard linkUp/linkDown traps defined in RFC are used.

- A standard linkUp trap is in the following format:

```
#Apr 24 11:48:04:896 2008 Sysname IFNET/4/INTERFACE UPDOWN:
 Trap 1.3.6.1.6.3.1.1.5.4<linkUp>: Interface 983555 is Up, ifAdminStatus is 1, ifOperStatus
is 1
```

- An extended linkUp trap is in the following format:

```
#Apr 24 11:43:09:896 2008 Sysname IFNET/4/INTERFACE UPDOWN:
 Trap 1.3.6.1.6.3.1.1.5.4<linkUp>: Interface 983555 is Up, ifAdminStatus is 1, ifOperStatus
is 1, ifDescr is GigabitEthernet1/0/1, ifType is 6
```

- A standard linkDown trap is in the following format:

```
#Apr 24 11:47:35:224 2008 Sysname IFNET/4/INTERFACE UPDOWN:
 Trap 1.3.6.1.6.3.1.1.5.3<linkDown>: Interface 983555 is Down, ifAdminStatus is 2,
ifOperStatus is 2
```

- An extended linkDown trap is in the following format:

```
#Apr 24 11:42:54:314 2008 AR29.46 IFNET/4/INTERFACE UPDOWN:
 Trap 1.3.6.1.6.3.1.1.5.3<linkDown>: Interface 983555 is Down, ifAdminStatus is 2,
ifOperStatus is 2, ifDescr is GigabitEthernet1/0/1, ifType is 6
```

The format of an extended linkup/ linkDown trap is the standard format followed with the ifDescr and ifType information, facilitating problem location.

Note that after this command is configured, the device sends extended linkUp/linkDown traps. If the extended messages are not supported on NMS, the device may not be able to resolve the messages.

Examples

Extend standard linkUp/linkDown traps defined in RFC.

```
<Sysname> system-view
[Sysname] snmp-agent trap if-mib link extended
```

snmp-agent trap life

Syntax

snmp-agent trap life *seconds*

undo snmp-agent trap life

View

System view

Default Level

3: Manage level

Parameters

seconds: Timeout time, in the range 1 to 2,592,000 seconds.

Description

Use the **snmp-agent trap life** command to configure the holding time of the traps in the queue. Traps will be discarded when the holding time expires.

Use the **undo snmp-agent trap life** command to restore the default holding time of traps in the queue.

By default, the holding time of SNMP traps in the queue is 120 seconds.

The SNMP module sends traps in queues. As soon as the traps are saved in the trap queue, a timer is started. If traps are not sent out until the timer times out (namely, the holding time configured by using this command expires), the system removes the traps from the trap sending queue.

Related commands: snmp-agent trap enable, snmp-agent target-host.

Examples

Configure the holding time of traps in the queue as 60 seconds.

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

snmp-agent trap queue-size

Syntax

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

View

System view

Default Level

3: Manage level

Parameters

size: Number of traps that can be stored in the trap sending queue, in the range 1 to 1,000.

Description

Use the **snmp-agent trap queue-size** command to set the size of the trap sending queue.

Use the **undo snmp-agent trap queue-size** command to restore the default queue size.

By default, up to 100 traps can be stored in the trap sending queue.

After traps are generated, they will be saved into the trap sending queue. The size of the queue determines the maximum number of the traps that can be stored in the queue. When the size of the trap sending queue reaches the configured value, the newly generated traps are saved into the queue, and the earliest ones are discarded.

Related commands: snmp-agent trap enable, snmp-agent target-host, snmp-agent trap life.

Examples

Set the maximum number of traps that can be stored in the trap sending queue to 200.

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

snmp-agent trap source

Syntax

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

undo snmp-agent trap source

View

System view

Default Level

3: Manage level

Parameters

interface-type interface-number: Specifies the interface type and interface number.

Description

Use the **snmp-agent trap source** command to specify the source IP address contained in the trap.

Use the **undo snmp-agent trap source** command to restore the default.

By default, SNMP chooses the IP address of an interface to be the source IP address of the trap.

Upon the execution of this command, the system uses the primary IP address of the specified interface as the source IP address of the traps, and the NMS will use this IP address to uniquely identify the agent. Even if the agent sends out traps through different interfaces, the NMS uses this IP address to filter all traps sent from the agent.

Use this command to trace a specific event by the source IP address of a trap.

Note that:

Before you can configure the IP address of a particular interface as the source IP address of the trap, ensure that the interface already exists and that it has a legal IP address. Otherwise, if the configured interface does not exist, the configurations will fail; if the specified IP address is illegal, the configuration will be invalid. After a legal IP address is configured for the interface, the configuration becomes valid automatically.

Related commands: **snmp-agent trap enable, snmp-agent target-host**.

Examples

Configure the IP address of Vlan-interface 1 as the source address for traps.

```
<Sysname> system-view
[Sysname] snmp-agent trap source Vlan-interface 1
```

snmp-agent usm-user { v1 | v2c }

Syntax

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*]

undo snmp-agent usm-user { v1 | v2c } *user-name group-name*

View

System view

Default Level

3: Manage level

Parameters

v1: The configured user name should be applied in the SNMPv1 networking environment. If the agent and the NMS use SNMPv1 packets to communicate with each other, this keyword is needed.

v2c: The configured user name should be applied in the SNMPv2c networking environment. If the agent and the NMS use SNMPv2c packets to communicate with each other, this keyword is needed.

user-name: User name, a string of 1 to 32 characters. It is case sensitive.

group-name: Group name, a string of 1 to 32 characters. It is case sensitive.

acl *acl-number*: Associates a basic ACL with the user. *acl-number* is in the range 2000 to 2999. By using a basic ACL, you can restrict the source IP address of SNMP packets, that is, you can configure to allow or prohibit SNMP packets with a specific source IP address, so as to allow or prohibit the specified NMS to access the agent by using this user name.

Description

Use the **snmp-agent usm-user** { **v1** | **v2c** } command to add a user to an SNMP group.

Use the **undo snmp-agent usm-user** { **v1** | **v2c** } command to delete a user from an SNMP group.

As defined in the SNMP protocol, in SNMPv1 and SNMPv2c networking applications, the NMS and the agent use community name to authenticate each other; in SNMPv3 networking applications, they use user name to authenticate each other. If you prefer using the user name in the authentication, the device supports configuration of SNMPv1 and SNMPv2c users. Creating an SNMPv1 or SNMPv2c user equals adding of a new read-only community name. After you add the user name into the read-only community name field of the NMS, the NMS can establish SNMP connection with the device.

To make the configured user take effect, create an SNMP group first.

Related commands: snmp-agent group, snmp-agent community, snmp-agent usm-user v3.

Examples

Create a v2c user **userv2c** in group **readCom**.

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom
```

- Set the SNMP version on the NMS to SNMPv2c
- Fill in the read community name **userv2c**, and then the NMS can access the agent

Create a v2c user **userv2c** in group **readCom**, allowing only the NMS with the IP address of 1.1.1.1 to access the agent by using this user name; other NMSs are not allowed to access the agent by using this user name.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[Sysname-acl-basic-2001] rule deny source any
[Sysname-acl-basic-2001] quit
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent group v2c readCom
[Sysname] snmp-agent usm-user v2c userv2c readCom acl 2001
```

- Set the IP address of the NMS to 1.1.1.1
- Set the SNMP version on the NMS to SNMPv2c
- Fill in both the read community and write community options with **userv2c**, and then the NMS can access the agent.

snmp-agent usm-user v3

Syntax

snmp-agent usm-user v3 *user-name group-name* [**cipher**] [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** *acl-number*]

undo snmp-agent usm-user v3 *user-name group-name* { **local** | **engineid** *engineid-string* }

View

System view

Default Level

3: Manage level

Parameters

user-name: User name, a string of 1 to 32 characters. It is case sensitive.

group-name: Group name, a string of 1 to 32 characters. It is case sensitive.

cipher: Specifies that *auth-password* and *priv-password* are cipher text passwords, which can be calculated by using the **snmp-agent calculate-password** command.

authentication-mode: Specifies the security model to be authentication. MD5 is faster than SHA, while SHA provides a higher security than MD5.

- **md5**: Specifies the authentication protocol as MD5.
- **sha**: Specifies the authentication protocol as SHA-1.

auth-password: Authentication password. If the **cipher** keyword is not specified, *auth-password* indicates a plain text password, which is a string of 1 to 64 visible characters. If the **cipher** keyword is specified, *auth-password* indicates a cipher text password. If the **md5** keyword is specified, *auth-password* is a string of 32 hexadecimal characters. If the **sha** keyword is specified, *auth-password* is a string of 40 hexadecimal characters.

privacy-mode: Specifies the security model to be privacy. The three encryption algorithms AES, 3DES, and DES are in descending order in terms of security. Higher security means more complex implementation mechanism and lower speed. DES is enough to meet general requirements.

- **3des**: Specifies the privacy protocol as 3DES.
- **des56**: Specifies the privacy protocol as DES.
- **aes128**: Specifies the privacy protocol as AES.

priv-password: The privacy password. If the **cipher** keyword is not specified, *priv-password* indicates a plain text password, which is a string of 1 to 64 characters; if the **cipher** keyword is specified, *priv-password* indicates a cipher text password; if the **3des** keyword is specified, *priv-password* is a string of 80 hexadecimal characters; if the **aes128** keyword is specified, *priv-password* is a string of 40 hexadecimal characters; if the **des56** keyword is specified, *priv-password* is a string of 40 hexadecimal characters.

acl *acl-number*: Associates a basic ACL with the user. *acl-number* is in the range 2000 to 2999. By using a basic ACL, you can restrict the source IP address of SNMP packets, that is, you can configure to allow or prohibit SNMP packets with a specific source IP address, so as to allow or prohibit the specified NMS to access the agent by using this user name.

local: Represents a local SNMP entity user.

engineid *engineid*-string: The engine ID string, an even number of hexadecimal characters, in the range 10 to 64. Its length must not be an odd number, and the all-zero and all-F strings are invalid.

Description

Use the **snmp-agent usm-user v3** command to add a user to an SNMP group.

Use the **undo snmp-agent usm-user v3** command to delete a user from an SNMP group.

The user name configured by using this command is applicable to the SNMPv3 networking environments, If the agent and the NMS use SNMPv3 packets to communicate with each other, you need to create an SNMPv3 user.

To make the configured user valid, create an SNMP group first. Configure the authentication and encryption modes when you create a group, and configure the authentication and encryption passwords when you create a user.

- If you specify the **cipher** keyword, the system considers the arguments *auth-password* and *priv-password* as cipher text passwords. In this case, the command supports copy and paste, meaning if the engine IDs of the two devices are the same, you can copy and paste the SNMPv3 configuration commands in the configuration file on device A to device B and execute the commands on device B. The cipher text password and plain text password on the two devices are the same.

- If you do not specify the **cipher** keyword, the system considers the arguments *auth-password* and *priv-password* as plain text passwords. In this case, if you perform the copy and paste operation, the system will encrypt these two passwords, resulting in inconsistency of the cipher text and plain text passwords of the two devices.

Note that:

- If you use the **snmp-agent usm-user v3 cipher** command, the *pri-password* argument in this command can be obtained by the **snmp-agent calculate-password** command. To make the calculated cipher text password applicable to the **snmp-agent usm-user v3 cipher** command and have the same effect as that in the **snmp-agent usm-user v3 cipher** command, ensure that the same privacy protocol is specified for the two commands and the local engine ID specified in the **snmp-agent usm-user v3 cipher** command is consistent with the SNMP entity engine ID specified in the **snmp-agent calculate-password** command.
- If you execute this command repeatedly to configure the same user (namely, the user names are the same, no limitation to other keywords and arguments), the last configuration takes effect.
- A plain text password is required when the NMS accesses the device; therefore, please remember the user name and the plain text password when you create a user.

Related commands: snmp-agent calculate-password, snmp-agent group, snmp-agent usm-user { v1 | v2c }.

Examples

Add a user **testUser** to the SNMPv3 group **testGroup**. Configure the security model as **authentication without privacy**, the authentication protocol as **MD5**, the plain-text authentication password as **authkey**.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup authentication
[Sysname] snmp-agent usm-user v3 testUser testGroup authentication-mode md5 authkey
```

- Set the SNMP version on the NMS to SNMPv3
- Fill in the user name **testUser**,
- Set the authentication protocol to **MD5**
- Set the authentication password to **authkey**
- Establish a connection, and the NMS can access the MIB objects in the ViewDefault view on the device

Add a user **testUser** to the SNMPv3 group **testGroup**. Configure the security model as **authentication and privacy**, the authentication protocol as MD5, the privacy protocol as DES56, the plain-text authentication password as **authkey**, and the plain-text privacy password as **prikey**.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent usm-user v3 testUser testGroup authentication-mode md5 authkey
privacy-mode des56 prikey
```

- Set the SNMP version on the NMS to SNMPv3
- Fill in the user name **testUser**,
- Set the authentication protocol to **MD5**
- Set the authentication password to **authkey**
- Set the privacy protocol to **DES**
- Set the privacy password to **prikey**

- Establish a connection, and the NMS can access the MIB objects in the ViewDefault view on the device

Add a user **testUser** to the SNMPv3 group **testGroup** with the **cipher** keyword specified. Configure the security model as **authentication and privacy**, the authentication protocol as MD5, the privacy protocol as DES56, the plain-text authentication password as **authkey**, and the plain-text privacy password as **prikey**

```
<Sysname> system-view
[Sysname] snmp-agent group v3 testGroup privacy
[Sysname] snmp-agent calculate-password authkey mode md5 local-engineid
The secret key is: 09659EC5A9AE91BA189E5845E1DDE0CC
[Sysname] snmp-agent calculate-password prikey mode md5 local-engineid
The secret key is: 800D7F26E786C4BECE61BF01E0A22705
[Sysname] snmp-agent usm-user v3 testUser testGroup cipher authentication-mode md5
09659EC5A9AE91BA189E5845E1DDE0CC privacy-mode des56 800D7F26E786C4BECE61BF01E0A22705
```

- Set the SNMP version on the NMS to SNMPv3
- Fill in the user name **testUser**,
- Set the authentication protocol to **MD5**
- Set the authentication password to **authkey**
- Set the privacy protocol to **DES**
- Set the privacy password to **prikey**
- Establish a connection, and the NMS can access the MIB objects in the ViewDefault view on the device

11 MIB Configuration Commands

MIB Configuration Commands

display mib-style

Syntax

display mib-style

View

Any view

Default Level

3: Manage level

Parameters

None

Description

Use the **display mib-style** command to display the MIB style of the device.

Two MIB styles are available on the device: **new** and **compatible**. After obtaining the MIB style, you can select matched 3Com network management software based on the MIB style.

Related commands: **mib-style**.

Examples

After getting the device ID from node **sysObjectID**, you find that it is an 3Com device, and hope to know the current MIB style or the MIB style after next boot of the device.

```
<Sysname> display mib-style
 Current MIB style: new
 Next reboot MIB style: new
```

The above output information indicates that the current MIB style of the device is **new**, and the MIB style after next boot is still **new**.

mib-style

Syntax

mib-style [**new** | **compatible**]

View

System view

Default Level

3: Manage level

Parameters

new: Specifies the MIB style of the device as 3Com **new**; that is, both sysOID and private MIB of the device are located under the 3Com enterprise ID 25506.

compatible: Specifies the MIB style of the device as 3Com **compatible**; that is, sysOID of the device is located under the 3Com enterprise ID 25506, and private MIB is located under the enterprise ID 2011.

Description

Use the **mib-style** command to set the MIB style of the device.

By default, the MIB style of the device is **new**.

Note that the configuration takes effect only after the device reboots.

Examples

Modify the MIB style of the device as **compatible**.

```
<Sysname> system-view
[Sysname] mib-style compatible
[Sysname] quit
<Sysname> display mib-style
 Current MIB style: new
 Next reboot MIB style: compatible
<Sysname> reboot
```

12 RMON Configuration Commands

RMON Configuration Commands

display rmon alarm

Syntax

display rmon alarm [*entry-number*]

View

Any view

Default Level

1: Monitor level

Parameters

entry-number: Index of an RMON alarm entry, in the range 1 to 65535. If no entry is specified, the configuration of all alarm entries is displayed.

Description

Use the **display rmon alarm** command to display the configuration of the specified or all RMON alarm entries.

Related commands: **rmon alarm**.

Examples

Display the configuration of all RMON alarm table entries.

```
<Sysname> display rmon alarm
AlarmEntry 1 owned by user1 is VALID.
  Samples type         : absolute
  Variable formula     : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval    : 10(sec)
  Rising threshold     : 50(linked with event 1)
  Falling threshold    : 5(linked with event 2)
  When startup enables  : risingOrFallingAlarm
  Latest value         : 0
```

Table 12-1 display rmon alarm command output description

Field	Description
AlarmEntry	Alarm entry, corresponding to the management information base (MIB) node alarmIndex.
owned by	Owner of the entry, user1 in this example, corresponding to the MIB node alarmOwner.

Field	Description
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry, while with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.), corresponding to the MIB node alarmStatus.
Samples type	The sampling type (the value can be absolute or delta), corresponding to the MIB node alarmSampleType.
Variable formula	Alarm variable, namely, the monitored MIB node, corresponding to the MIB node alarmVariable.
Sampling interval	Sampling interval, in seconds, corresponding to the MIB node alarmInterval.
Rising threshold	Alarm rising threshold (When the sampling value is bigger than or equal to this threshold, a rising alarm is triggered.), corresponding to the MIB node alarmRisingThreshold.
Falling threshold	Alarm falling threshold (When the sampling value is smaller than or equal to this threshold, a falling alarm is triggered.), corresponding to the MIB node alarmFallingThreshold.
When startup enables	How an alarm can be triggered, corresponding to the MIB node alarmStartupAlarm.
Latest value	The last sampled value, corresponding to the MIB node alarmValue.

display rmon event

Syntax

display rmon event [*entry-number*]

View

Any view

Default Level

1: Monitor level

Parameters

entry-number: Index of an RMON event entry, in the range 1 to 65535. If no entry is specified, the configuration of all event entries is displayed.

Description

Use the **display rmon event** command to display the configuration of the specified or all RMON event entries.

Displayed information includes event index, event owner, event description, action triggered by the event (such as sending log or trap messages), and last time the event occurred (the elapsed time since system initialization/startup) in seconds.

Related commands: **rmon event**.

Examples

Display the configuration of RMON event table.

```
<Sysname> display rmon event
EventEntry 1 owned by user1 is VALID.
  Description: null.
  Will cause log-trap when triggered, last triggered at 0days 00h:02m:27s.
```

Table 12-2 display rmon event command output description

Field	Description
EventEntry	Event entry, corresponding to the MIB node eventIndex.
owned by	Owner of the entry, corresponding to the MIB node eventOwner.
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry; while with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.), corresponding to the MIB node eventStatus.
Description	Description for the event, corresponding to the MIB node eventDescription.
cause log-trap when triggered	The actions that the system will take when the event is triggered: • none: The system will take no action • log: The system will log the event • snmp-trap: The system will send a trap to the NMS • log-and-trap: The system will log the event and send a trap to the NMS This field corresponds to the MIB node eventType.
last triggered at	Time when the last event was triggered, corresponding to the MIB node eventLastTimeSent.

display rmon eventlog

Syntax

display rmon eventlog [*entry-number*]

View

Any view

Default Level

1: Monitor level

Parameters

entry-number: Index of an event entry, in the range 1 to 65535.

Description

Use the **display rmon eventlog** command to display log information for the specified or all event entries.

If *entry-number* is not specified, the log information for all event entries is displayed.

If you use the **rmon event** command to configure the system to log an event when the event is triggered, the event is recorded into the RMON log. You can use this command to display the details of the log table: event index, current event state, time the event was logged (the elapsed time in seconds since system initialization/startup), and event description.

Examples

Display the RMON log information for event entry 1.

```
<Sysname> display rmon eventlog 1
LogEntry 1 owned by null is VALID.
  Generates eventLog 1.1 at 0day(s) 00h:00m:33s.
  Description: The alarm formula defined in prialarmEntry 1,
    uprise 80 with alarm value 85. Alarm sample type is absolute.
  Generates eventLog 1.2 at 0day(s) 00h:42m:03s.
  Description: The alarm formula defined in prialarmEntry 2,
    less than(or =) 5 with alarm value 0. Alarm sample type is delta.
```

Table 12-3 display rmon eventlog command output description

Field	Description
LogEntry	Event log entry, corresponding to the MIB node logIndex.
owned by	Owner of the entry, corresponding to the MIB node eventOwner.
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry; while with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.), corresponding to the MIB node eventStatus.
Generates eventLog at	Time when the log was created (Time passed since the device was booted), corresponding to the MIB node logTime.
Description	Log description, corresponding to the MIB node logDescription.

The above example shows that event 1 has generated two logs:

- eventLog 1.1, generated by private alarm entry 1, which is triggered because the alarm value (85) exceeds the rising threshold (80). The sampling type is **absolute**.
- eventLog 1.2, generated by private alarm entry 2, which is triggered because the alarm value (0) is lower than the falling threshold (5). The sampling type is **delta**.

display rmon history

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Description

Use the **display rmon history** command to display RMON history control entry and history sampling information.

After you have created history control entry on an interface, the system calculates the information of the interface periodically and saves this information to the etherHistoryEntry table. You can use this command to display the entries in this table.

You can configure the number of history sampling records that can be displayed and the history sampling interval through the **rmon history** command.

Related commands: **rmon history**.

Examples

Display RMON history control entry and history sampling information for interface GigabitEthernet 1/0/1.

```
<Sysname> display rmon history GigabitEthernet 1/0/1
HistoryControlEntry 1 owned by null is VALID
  Samples interface    : GigabitEthernet1/0/1<ifIndex.1>
  Sampling interval    : 10(sec) with 5 buckets max
  Sampled values of record 1 :
    dropevents       : 0        , octets             : 0
    packets          : 0        , broadcast packets    : 0
    multicast packets : 0         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
    fragments        : 0        , jabbers            : 0
    collisions       : 0        , utilization         : 0
  Sampled values of record 2 :
    dropevents       : 0        , octets             : 0
    packets          : 0        , broadcast packets    : 0
    multicast packets : 0         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
    fragments        : 0        , jabbers            : 0
    collisions       : 0        , utilization         : 0
  Sampled values of record 3 :
    dropevents       : 0        , octets             : 0
    packets          : 0        , broadcast packets    : 0
    multicast packets : 0         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
    fragments        : 0        , jabbers            : 0
    collisions       : 0        , utilization         : 0
  Sampled values of record 4 :
    dropevents       : 0        , octets             : 0
    packets          : 0        , broadcast packets    : 0
    multicast packets : 0         , CRC alignment errors : 0
    undersize packets : 0         , oversize packets     : 0
```

```
  fragments        : 0        , jabbers            : 0
  collisions       : 0        , utilization        : 0
Sampled values of record 5 :
  dropevents       : 0        , octets             : 0
  packets          : 0        , broadcast packets  : 0
  multicast packets : 0         , CRC alignment errors : 0
  undersize packets : 0         , oversize packets    : 0
  fragments        : 0        , jabbers            : 0
  collisions       : 0        , utilization        : 0
```

Table 12-4 display rmon history command output description

Field	Description
HistoryControlEntry	History control entry, corresponding to the MIB node etherHistoryIndex.
owned by	Owner of the entry, corresponding to the MIB node historyControlOwner.
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry; while with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.), corresponding to the MIB node historyControlStatus.
Samples Interface	The sampled interface
Sampling interval	Sampling period, in seconds, corresponding to the MIB node historyControlInterval. The system samples the information of an interface periodically.
buckets max	The maximum number of history table entries that can be saved, corresponding to the MIB node historyControlBucketsGranted. If the specified value of the **buckets** argument exceeds the history table size supported by the device, the supported history table size is displayed. If the current number of the entries in the table has reached the maximum number, the system will delete the earliest entry to save the latest one.
Sampled values of record *number*	The (*number*)th statistics recorded in the system cache. Statistics records are numbered according to the order of time they are saved into the cache.
dropevents	Dropped packets during the sampling period, corresponding to the MIB node etherHistoryDropEvents.
octets	Number of octets received during the sampling period, corresponding to the MIB node etherHistoryOctets.
packets	Number of packets received during the sampling period, corresponding to the MIB node etherHistoryPkts.
broadcastpackets	Number of broadcasts received during the sampling period, corresponding to the MIB node etherHistoryBroadcastPkts.
multicastpackets	Number of multicasts received during the sampling period, corresponding to the MIB node etherHistoryMulticastPkts.

Field	Description
CRC alignment errors	Number of packets received with CRC alignment errors during the sampling period, corresponding to the MIB node etherHistoryCRCAlignErrors.
undersize packets	Number of undersize packets received during the sampling period, corresponding to the MIB node etherHistoryUndersizePkts.
oversize packets	Number of oversize packets received during the sampling period, corresponding to the MIB node etherHistoryOversizePkts.
fragments	Number of fragments received during the sampling period, corresponding to the MIB node etherHistoryFragments.
jabbers	Number of jabbers received during the sampling period corresponding to the MIB node etherHistoryJabbers.
collisions	Number of colliding packets received during the sampling period, corresponding to the MIB node etherHistoryCollisions.
utilization	Bandwidth utilization during the sampling period, corresponding to the MIB node etherHistoryUtilization.

display rmon prialarm

Syntax

display rmon prialarm [*entry-number*]

View

Any view

Default Level

1: Monitor level

Parameters

entry-number: Private alarm entry index, in the range 1 to 65535. If no entry is specified, the configuration of all private alarm entries is displayed.

Description

Use the **display rmon prialarm** command to display the configuration of the specified or all private alarm entries.

Related commands: **rmon prialarm**.

Examples

Display the configuration of all private alarm entries.

```
<Sysname> display rmon prialarm
PrialarmEntry 1 owned by user1 is VALID.
  Samples type         : absolute
  Variable formula      : (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
  Description          : ifUtilization.GigabitEthernet1/0/1
```

```
Sampling interval     : 10(sec)
Rising threshold      : 80(linked with event 1)
Falling threshold     : 5(linked with event 2)
When startup enables  : risingOrFallingAlarm
This entry will exist : forever
Latest value          : 85
```

Table 12-5 display rmon prialarm command output description

Field	Description
PrialarmEntry	The entry of the private alarm table
owned by	Owner of the entry, user1 in this example
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry; while with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.)
Samples type	Sampling type, whose value can be absolute or delta.
Sampling interval	Sampling interval, in seconds. The system performs absolute sample or delta sample to sampling variables according to the sampling interval.
Rising threshold	Alarm rising threshold. An event is triggered when the sampled value is greater than or equal to this threshold.
Falling threshold	Alarm falling threshold. An event is triggered when the sampled value is less than or equal to this threshold.
linked with event	Event index associated with the prialarm
When startup enables	How can an alarm be triggered
This entry will exist	The lifetime of the entry, which can be forever or span the specified period
Latest value	The count result of the last sample

display rmon statistics

Syntax

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

View

Any view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Description

Use the **display rmon statistics** command to display RMON statistics.

This command displays the interface statistics during the period from the time the statistics entry is created to the time the command is executed. The statistics are cleared after the device reboots.

Related commands: **rmon statistics**.

Examples

Display RMON statistics for interface GigabitEthernet 1/0/1.

```
<Sysname> display rmon statistics GigabitEthernet 1/0/1
EtherStatsEntry 1 owned by null is VALID.
  Interface : GigabitEthernet1/0/1<ifIndex.3>
  etherStatsOctets        : 43393306  , etherStatsPkts        : 619825
  etherStatsBroadcastPkts  : 503581    , etherStatsMulticastPkts : 44013
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Packets received according to length:
  64     : 0         ,  65-127  : 0         ,  128-255  : 0
  256-511: 0         ,  512-1023: 0         ,  1024-1518: 0
```

Table 12-6 display rmon statistics command output description

Field	Description
EtherStatsEntry	The entry of the statistics table, corresponding to the MIB node etherStatsIndex.
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry; while with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.), corresponding to the MIB node etherStatsStatus.
Interface	Interface on which statistics are gathered, corresponding to the MIB node etherStatsDataSource.
etherStatsOctets	Number of octets received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsOctets.
etherStatsPkts	Number of packets received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsPkts.
etherStatsBroadcastPkts	Number of broadcast packets received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsBroadcastPkts.
etherStatsMulticastPkts	Number of multicast packets received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsMulticastPkts.
etherStatsUndersizePkts	Number of undersize packets received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsUndersizePkts.
etherStatsOversizePkts	Number of oversize packets received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsOversizePkts.

Field	Description
etherStatsFragments	Number of undersize packets with CRC errors received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsFragments.
etherStatsJabbers	Number of oversize packets with CRC errors received and sent by the interface during the statistical period, corresponding to the MIB node etherStatsJabbers.
etherStatsCRCAlignErrors	Number of packets with CRC errors received and sent on the interface during the statistical period, corresponding to the MIB node etherStatsCRCAlignErrors.
etherStatsCollisions	Number of collisions received and sent on the interface during the statistical period, corresponding to the MIB node etherStatsCollisions.
etherStatsDropEvents	Total number of drop events received and sent on the interface during the statistical period, corresponding to the MIB node etherStatsDropEvents.
Packets received according to length: 64 : 0 , 65-127 : 0 , 128-255 : 0 256-511: 0 , 512-1023: 0 , 1024-1518: 0	Statistics of packets received and sent according to length during the statistical period (Hardware support is needed for the statistics. If the hardware does not support the function, all statistics are displayed as 0.), in which: • Information of the field 64 corresponds to the MIB node etherStatsPkts64Octets • Information of the field 65-127 corresponds to the MIB node etherStatsPkts65to127Octets • Information of the field 128-255 corresponds to the MIB node etherStatsPkts128to255Octets • Information of the field 256-511 corresponds to the MIB node etherStatsPkts256to511Octets • Information of the field 512-1023 corresponds to the MIB node etherStatsPkts512to1023Octets • Information of the field 1024-1518 corresponds to the MIB node etherStatsPkts1024to1518Octets

rmon alarm

Syntax

rmon alarm *entry-number alarm-variable sampling-interval* { **absolute** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*]

undo rmon alarm *entry-number*

View

System view

Default Level

2: System level

Parameters

entry-number: Alarm entry index, in the range 1 to 65535.

alarm-variable: Alarm variable, a string of 1 to 256 characters. It can be in dotted object identifier (OID) format (in the format of *entry.integer.instance* or *leaf node name.instance*, for example,

1.3.6.1.2.1.2.1.10.1), or a node name like ifInOctets.1. Only variables that can be parsed into INTEGER (INTEGER, Counter, Gauge, or Time Ticks) in the ASN.1 can be used for the *alarm-variable* argument, such as the instance of the leaf node (like etherStatsOctets, etherStatsPkts, etherStatsBroadcastPkts, and so on) of the etherStatsEntry entry, the instance of the leaf node (like ifInOctets, ifInUcastPkts, ifInNUcastPkts, and so on) of the ifEntry entry.

sampling-interval: Sampling interval, in the range 5 to 65,535 seconds.

absolute: Sets the sampling type to **absolute**, namely, the system obtains the value of the variable when the sampling time is reached.

delta: Sets the sampling type to **delta**, namely, the system obtains the variation value of the variable during the sampling interval when the sampling time is reached.

rising-threshold *threshold-value1 event-entry1*: Sets the rising threshold, where *threshold-value1* represents the rising threshold, in the range –2,147,483,648 to +2,147,483,647, and *event-entry1* represents the index of the event triggered when the rising threshold is reached. *event-entry1* ranges from 0 to 65,535, with 0 meaning no corresponding event is triggered and no event action is taken when an alarm is triggered.

falling-threshold *threshold-value2 event-entry2*: Sets the falling threshold, where *threshold-value2* represents the falling threshold, in the range –2,147,483,648 to +2,147,483,647 and *event-entry2* represents the index of the event triggered when the falling threshold is reached. *event-entry2* ranges from 1 to 65,535.

owner *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description

Use the **rmon alarm** command to create an entry in the RMON alarm table.

Use the **undo rmon alarm** command to remove a specified entry from the RMON alarm table.

This command defines an alarm entry, so as to trigger the specified event when abnormity occurs. The event defines how to deal with the abnormity.

The following is how the system handles alarm entries:

1) Samples the alarm variables at the specified interval.
2) Compares the sampled values with the predefined threshold and does the following:

- If the rising threshold is reached, triggers the event specified by the *event-entry1* argument.
- If the falling threshold is reached, triggers the event specified by the *event-entry2* argument.

Note

- Before creating an alarm entry, define the events to be referenced in the event table with the **rmon event** command.
- When you create an entry, if the values of the specified alarm variable (*alarm-variable*), sampling interval (*sampling-interval*), sampling type (**absolute** or **delta**), rising threshold (*threshold-value1*) and falling threshold (*threshold-value2*) are identical to those of the existing alarm entry, the system considers their configurations are the same and the creation fails.
- You can create up to 60 alarm entries.

Related commands: **display rmon alarm**, **rmon event**, **rmon history**, **rmon statistics**.

Examples

Add entry 1 in the alarm table and sample the node 1.3.6.1.2.1.16.1.1.1.4.1 at a sampling interval of 10 seconds in absolute sampling type. Trigger event 1 when the sampled value is greater than or equal to the rising threshold of 5000, and event 2 when the sampled value is less than or equal to the falling threshold of 5. Set the owner of the entry to be **user1**.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising-threshold 5000 1
falling-threshold 5 2 owner user1
```

1.3.6.1.2.1.16.1.1.1.4 is the OID of the leaf node etherStatsOctets. It represents the statistics of the received packets on the interface, in bytes. In the above example, you can use etherStatsOctets.1 to replace the parameter 1.3.6.1.2.1.16.1.1.1.4.1, where 1 indicates the serial number of the interface statistics entry. Therefore, if you execute the **rmon statistics 5** command, you can use etherStatsOctets.5 to replace the parameter.

The above configuration implements the following:

- Sampling and monitoring interface GigabitEthernet 1/0/1
- Obtaining the absolute value of the number of received packets. If the total bytes of the received packets reach 5,000, the system will log the event; if the total bytes of the received packets are no more than 5, the system will take no action.

rmon event

Syntax

rmon event *entry-number* [**description** *string*] { **log** | **log-trap** *log-trapcommunity* | **none** | **trap** *trap-community* } [**owner** *text*]

undo rmon event *entry-number*

View

System view

Default Level

2: System level

Parameters

entry-number: Event entry index, in the range 1 to 65,535.

description *string*: Event description, a string of 1 to 127 characters.

log: Logs the event when it occurs.

log-trap *log-trapcommunity*: Log and trap events. The system performs both logging and trap sending when the event occurs. *log-trapcommunity* indicates the community name of the network management station that receives trap messages, a string of 1 to 127 characters.

none: Performs no action when the event occurs.

trap *trap-community*: Trap event. The system sends a trap with a community name when the event occurs. *trap-community* specifies the community name of the network management station that receives trap messages, a string of 1 to 127 characters.

owner *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description

Use the **rmon event** command to create an entry in the RMON event table.

Use the **undo rmon event** command to remove a specified entry from the RMON event table.

When create an event entry, you can define the actions that the system will take when the event is triggered by its associated alarm in the alarm table. According to your configuration, the system can log the event, send a trap, do both, or do neither at all.

Related commands: **display rmon event**, **rmon alarm**, **rmon prialarm**.

Note

- When you create an entry, if the values of the specified event description (**description** *string*), event type (**log**, **trap**, **logtrap** or **none**), and community name (*trap-community* or *log-trapcommunity)* are identical to those of the existing event entry, the system considers their configurations are the same and the creation fails.
- You can create up to 60 alarm entries.

Examples

Create event 10 in the RMON event table.

```
<Sysname> system-view
[Sysname] rmon event 10 log owner user1
```

rmon history

Syntax

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

undo rmon history *entry-number*

View

Ethernet interface view

Default Level

2: System level

Parameters

entry-number: History control entry index, in the range 1 to 65535.

buckets *number*: History table size for the entry, in the range 1 to 65,535.

interval *sampling-interval*: Sampling period, in the range 5 to 3600 seconds.

owner *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description

Use the **rmon history** command to create an entry in the RMON history control table.

Use the **undo rmon history** command to remove a specified entry from the RMON history control table.

After an entry is created, the system periodically samples the number of packets received/sent on the current interface, and saves the statistics as an instance under the leaf node of the etherHistoryEntry table. The maximum number of history entries can be saved in the table is specified by **buckets** *number*. If the number of the entries in the table has reached the maximum number, the system will delete the earliest entry to save the latest one. The statistics include total number of received packets on the current interface, total number of broadcast packets, and total number of multicast packets in a sampling period,

When you create an entry in the history table, if the specified history table size exceeds that supported by the device, the entry will be created. However, the validated value of the history table size corresponding to the entry is that supported by the device. You can use the **display rmon history** command to view the configuration result.

Note

- When you create an entry, if the value of the specified sampling interval (**interval** *sampling-interval*) is identical to that of the existing history entry, the system considers their configurations are the same and the creation fails.
- You can create up to 100 alarm entries.

Related commands: **display rmon history**.

Examples

Create RMON history control entry 1 for interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon history 1 buckets 10 interval 5 owner user1
```

rmon prialarm

Syntax

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

undo rmon prialarm *entry-number*

View

System view

Default Level

2: System level

Parameters

entry-number: Index of a private alarm entry, in the range 1 to 65535.

prialarm-formula: Private alarm variable formula, a string of 1 to 256 characters. The variables in the formula must be represented in OID format that starts with a point ".", the formula (.1.3.6.1.2.1.2.1.10.1)*8 for example. You may perform the basic operations of addition, subtraction, multiplication, and division on these variables. The operations should yield a long integer. To prevent errors, make sure that the result of each calculating step falls into the value range for long integers.

prialarm-des: Private alarm entry description, a string of 1 to 127 characters.

sampling-interval: Sampling interval, in the range 10 to 65,535 seconds.

absolute | **changeratio** | **delta** : Sets the sampling type to absolute, delta, or change ratio. Absolute sampling is to obtain the value of the variable when the sampling time is reached; delta sampling is to obtain the variation value of the variable during the sampling interval when the sampling time is reached; change ratio sampling is not supported at present.

rising-threshold *threshold-value1 event-entry1*: Sets the rising threshold, where *threshold-value1* represents the rising threshold, in the range –2,147,483,648 to +2,147,483,647, and *event-entry1* represents the index of the event triggered when the rising threshold is reached. *event-entry1* ranges from 0 to 65,535, with 0 meaning no corresponding event is triggered and no event action is taken when an alarm is triggered.

falling-threshold *threshold-value2 event-entry2*: Sets the falling threshold, where *threshold-value2* represents the falling threshold, in the range –2,147,483,648 to +2,147,483,647 and *event-entry2* represents the index of the event triggered when the falling threshold is reached. *event-entry2* ranges from 1 to 65,535.

forever: Indicates that the lifetime of the private alarm entry is infinite.

cycle *cycle-period*: Sets the lifetime period of the private alarm entry, in the range 0 to 2,147,483,647 seconds.

owner *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description

Use the **rmon prialarm** command to create an entry in the private alarm table of RMON.

Use the **undo rmon prialarm** command to remove a private alarm entry from the private alarm table of RMON.

The following is how the system handles private alarm entries:

1) Samples the private alarm variables in the private alarm formula at the specified sampling interval.
2) Performs calculation on the sampled values with the formula.
3) Compares the calculation result with the predefined thresholds and does the following:

- If the result is equal to or greater than the rising threshold, triggers the event specified by the *event-entry1* argument.

- If the result is equal to or smaller than the falling threshold, triggers the event specified by the *event-entry2* argument.

Note

- Before creating an alarm entry, define the events to be referenced in the event table with the **rmon event** command.
- When you create an entry, if the values of the specified alarm variable formula (*prialarm-formula*), sampling type (**absolute changeratio** or **delta**), rising threshold (*threshold-value1*) and falling threshold (*threshold-value2*) are identical to those of the existing alarm entry, the system considers their configurations are the same and the creation fails.
- You can create up to 50 pri-alarm entries.

Related commands: **display rmon prialarm**, **rmon event**, **rmon history**, **rmon statistics**.

Examples

Create entry 5 in the private alarm table. Calculate the private alarm variables with the (1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1) formula and sample the corresponding variables at intervals of 10 seconds. Rising threshold of 80 corresponds to event 1 (and record the event into the log table); falling threshold of 5 corresponds to event 2 (but neither log it nor send a trap). Set the lifetime of the entry to **forever** and owner to **user1**.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] rmon prialarm 1 (1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1)
packet GigabitEthernet1/0/1 10 absolute rising_threshold 80 1 falling_threshold 5 2 entrytype
forever owner user1
```

1.3.6.1.2.1.16.1.1.1.6.1 is the OID of the node etherStatsBroadcastPkts.1, and 1.3.6.1.2.1.16.1.1.1.5.1 is the OID of the node etherStatsPkts.1. 1 indicates the serial number of the interface statistics entry. Therefore, if you execute the **rmon statistics 5** command, you should use 1.3.6.1.2.1.16.1.1.1.6.5 and 1.3.6.1.2.1.16.1.1.1.5.5.

The above configuration implements the following:

- Sampling and monitoring interface GigabitEthernet1/0/1
- If the portion of broadcast packets received in the total packets is greater than or equal to 80%, the system will log the event; if the portion is less than or equal to 5%, the system will take no action.

You can view the event log using the **display rmon eventlog** command.

rmon statistics

Syntax

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

undo rmon statistics *entry-number*

View

Ethernet interface view

Default Level

2: System level

Parameters

entry-number: Index of statistics entry, in the range 1 to 65535.

owner *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description

Use the **rmon statistics** command to create an entry in the RMON statistics table.

Use the **undo rmon statistics** command to remove a specified entry from the RMON statistics table.

After an entry is created, the system continuously calculates the information of the interface. It provides statistics about network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, packets received, bytes sent, packets sent, and so on. The statistics are cleared after the device reboots.

To display information for the RMON statistics table, use the **display rmon statistics** command.

Note

- Only one statistics entry can be created on one interface.
- You can create up to 100 statistics entries.

Examples

Create an entry in the RMON statistics table for interface GigabitEthernet 1/0/1. The index of the entry is 20, and the owner of the entry is **user1**.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 20 owner user1
```

13 MAC Address Table Management Configuration Commands

Note

Interfaces that MAC address table management involves can only be Ethernet ports.

MAC Address Table Management Configuration Commands

display mac-address

Syntax

display mac-address blackhole [**vlan** *vlan-id*] [**count**]

display mac-address [*mac-address* [**vlan** *vlan-id*] | [**dynamic** | **static**] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]]

View

Any view

Default Level

1: Monitor level

Parameters

blackhole: Destination blackhole MAC address entries. These entries do not age but you can add or remove them. The packets whose destination MAC addresses match destination blackhole MAC address entries are dropped.

vlan *vlan-id*: Displays MAC address entries of the specified VLAN, where *vlan-id* is in the range 1 to 4094.

count: Displays the total number of MAC addresses in the MAC address table.

mac-address: Displays MAC address entries in a specified MAC address, in the format of H-H-H.

dynamic: Displays dynamic MAC address entries. Aging time is set for these entries.

static: Displays static MAC address entries. Similar to blackhole MAC address entries, these entries do not age but you can add or remove them.

interface *interface-type interface-number*: Displays MAC address learning status of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

Description

Use the **display mac-address** command to display information about the MAC address table.

Related commands: **mac-address (system view)**, **mac-address (Ethernet interface view)**, **mac-address timer**.

Examples

Display the MAC address table entry for MAC address 000f-e201-0101.

```
<Sysname> display mac-address 000f-e201-0101
MAC ADDR          VLAN ID  STATE      PORT INDEX            AGING TIME(s)
000f-e201-0101     1       Learned      GigabitEthernet1/0/1    AGING
```

Table 13-1 display mac-address command output description

Field	Description
MAC ADDR	MAC address
VLAN ID	ID of the VLAN to which the MAC address belongs
STATE	State of a MAC address, includes: • Config static: static entry configured by the user manually • Config dynamic: dynamic entry configured by the user manually • Learned: entry learned by the device • Blackhole: destination blackhole entry • Source-Blackhole: source blackhole entry
PORT INDEX	Number of the port corresponding to the MAC address, that is, packets destined to this MAC address will be sent out from this port. (Displayed as N/A for a blackhole MAC address entry).
AGING TIME(s)	Aging time, which could be: • *AGING, indicates that the entry is aging.* • *NOAGED, indicates that the entry does not age.*

display mac-address aging-time

Syntax

display mac-address aging-time

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display mac-address aging-time** command to display the aging time of dynamic entries in the MAC address table.

Related commands: **mac-address (system view)**, **mac-address (Ethernet interface view)**, **mac-address timer**, **display mac-address**.

Examples

Display the aging time of dynamic entries in the MAC address table.

```
<Sysname> display mac-address aging-time
Mac address aging time: 300s
```

The above information indicates that the aging time of dynamic entries in the MAC address table is 300 seconds.

mac-address (Interface view)

Syntax

mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

undo mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

View

Ethernet interface view, Layer-2 aggregate interface view

Default Level

2: System level

Parameters

dynamic: Dynamic MAC address entries. Aging time is set for these entries.

static: Static MAC address entries. They do not age but you can add or remove them.

mac-address: Specifies a MAC address in the format of H-H-H, where 0s at the beginning of each H (16-bit hexadecimal digit) can be omitted; for example, inputting “f-e2-1” indicates that the MAC address is “000f-00e2-0001”.

vlan *vlan-id*: Specifies an existing VLAN to which the Ethernet interface belongs, where *vlan-id* is the specified VLAN ID, in the range 1 to 4094.

Description

Use the **mac-address** command to add or modify a MAC address entry on a specified interface.

Use the **undo mac-address** command to remove a MAC address entry on the interface.

Note that, as your MAC address entries configuration cannot survive a reboot, save it after completing the configuration. The dynamic MAC address table entries however will be lost whether you save the configuration or not.

Related commands: **display mac-address**.

Examples

Add a static entry for MAC address 000f-e201-0101 on port GigabitEthernet 1/0/1 that belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address static 000f-e201-0101 vlan 2
```

Add a static entry for MAC address 000f-e201-0102 on port Bridge-Aggregation 1 that belongs to VLAN 1.

```
<Sysname> system-view
[Sysname] interface bridge-Aggregation 1
[Sysname-Bridge-Aggregation1] mac-address static 000f-e201-0102 vlan 1
```

mac-address (system view)

Syntax

mac-address blackhole *mac-address* **vlan** *vlan-id*

mac-address { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

undo mac-address [{ **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*]

undo mac-address [**blackhole** | **dynamic** | **static**] [*mac-address*] **vlan** *vlan-id*

undo mac-address [**dynamic** | **static**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

undo mac-address [**dynamic** | **static**] **interface** *interface-type interface-number*

View

System view

Default Level

2: System level

Parameters

blackhole: Destination blackhole MAC address entries. These entries do not age but you can add or remove them. The packets whose destination MAC addresses match destination blackhole MAC address entries are dropped.

mac-address: Specifies a MAC address in the format of H-H-H, where 0s at the beginning of each H (16-bit hexadecimal digit) can be omitted; for example, inputting “f-e2-1” indicates that the MAC address is “000f-00e2-0001”.

vlan *vlan-id*: Specifies an existing VLAN to which the Ethernet interface belongs, where *vlan-id* is the specified VLAN ID, in the range 1 to 4094.

dynamic: Dynamic MAC address entries. Aging time is set for these entries.

static: Static MAC address entries. These entries do not age but you can add or remove them.

interface *interface-type interface-number*: Outbound interface, with *interface-type interface-number* representing the interface type and number.

Description

Use the **mac-address** command to add or modify a MAC address entry.

Use the **undo mac-address** command to remove one or all MAC address entries.

Note that a static or blackhole entry will not be overwritten by a dynamic entry, but a dynamic entry can be overwritten by a static or blackhole entry. However, you can delete any type of MAC address entries.

As your MAC address entries configuration cannot survive a reboot, save it after completing the configuration. The dynamic entries however will be lost whether you save the configuration or not.

Related commands: **display mac-address**.

Examples

Add a static entry for MAC address 000f-e201-0101. All frames destined to this MAC address are sent out of port GigabitEthernet 1/0/1 which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address static 000f-e201-0101 interface gigabitethernet 1/0/1 vlan 2
```

mac-address mac-learning disable

Syntax

mac-address mac-learning disable

undo mac-address mac-learning disable

View

VLAN view

Default Level

2: System level

Parameters

None

Description

Use the **mac-address mac-learning disable** command to disable MAC address learning on a VLAN. Use the **undo mac-address mac-learning disable** command to enable MAC address learning on a VLAN.

By default, MAC address learning is enabled on all VLANs.

Note that:

- You may need to disable MAC address learning sometimes to prevent the MAC address table from being saturated, for example, when your device is being attacked by a great deal of packets with different source MAC addresses. This somewhat affects update of the MAC address table.
- As disabling MAC address learning may result in broadcast storms, you need to enable broadcast storm suppression after you disable MAC address learning on a port.

Related commands: **display mac-address mac-learning**.

Note

Once MAC learning is disabled in a VLAN, all MAC address entries learnt in the VLAN are removed.

Examples

Disable MAC address learning on VLAN 10.

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] mac-address mac-learning disable
```

mac-address max-mac-count (Interface view)

Syntax

mac-address max-mac-count *count*

undo mac-address max-mac-count

View

Ethernet interface view, port group view

Default Level

2: System level

Parameters

count: Maximum number of MAC addresses that can be learned on a port, ranging from 0 to 4096. When the argument takes 0, the VLAN is not allowed to learn MAC addresses.

disable-forwarding: Disables forwarding of frames with unknown source MAC addresses after the number of learned MAC addresses reaches the upper limit. Frames with the source MAC addresses listed in the MAC address table will be forwarded normally.

Description

Use the **mac-address max-mac-count** *count* command to configure the maximum number of MAC addresses that can be learned on an Ethernet port.

Use the **undo mac-address max-mac-count** command to restore the default maximum number of MAC addresses that can be learned on an Ethernet port.

By default, the maximum number of MAC addresses that can be learned on an Ethernet port is not configured.

If the command is executed in interface view, the configuration takes effect on the current interface; if the command is executed in port group view, the configuration takes effect on all ports belonging to the port group.

Related commands: **mac-address**, **mac-address timer**.

Examples

Set the maximum number of MAC addresses that can be learned on port GigabitEthernet 1/0/1 to 600. After this upper limit is reached, frames received with unknown source MAC addresses on the port will not be forwarded.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 600
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count disable-forwarding
```

mac-address timer

Syntax

mac-address timer { **aging** *seconds* | **no-aging** }

undo mac-address timer aging

View

System view

Default Level

2: System level

Parameters

aging *seconds*: Sets an aging timer in seconds for dynamic MAC address entries. The *seconds* argument ranges from 10 to 1000000.

no-aging: Sets dynamic MAC address entries not to age.

Description

Use the **mac-address timer** command to configure the aging timer for dynamic MAC address entries.

Use the **undo mac-address timer** command to restore the default.

By default the default aging timer is 300 seconds.

Set the aging timer appropriately: a long aging interval may cause the MAC address table to retain outdated entries and fail to accommodate the latest network changes; a short interval may result in removal of valid entries and hence unnecessary broadcasts which may affect device performance.

Examples

Set the aging timer for dynamic MAC address entries to 500 seconds.

```
<Sysname> system-view
[Sysname] mac-address timer aging 500
```

14 MAC Information Configuration Commands

Note

Currently, MAC Information applies to only Layer-2 Ethernet interfaces.

MAC Information Configuration Commands

mac-address information enable (Ethernet interface view)

Syntax

mac-address information enable { **added** | **deleted** }

undo mac-address information enable { **added** | **deleted** }

View

Ethernet interface view

Default Level

1: Monitor level

Parameters

added: Enables the device to record security information when a new MAC address is learned on the Ethernet port.

deleted: Enables the device to record security information when an existing MAC address is deleted.

Description

Use the **mac-address information enable** command to enable MAC Information on the Layer-2 Ethernet interface.

Use the **undo mac-address information enable** command to disable MAC Information on the Layer-2 Ethernet interface.

By default, MAC Information is disabled on a Layer-2 Ethernet interface.

Note that:

- This command is not supported on aggregate interfaces.
- To enable MAC Information on an Ethernet interface, enable MAC Information globally first.

Examples

Enable MAC Information on GigabitEthernet1/0/1.

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address information enable added
```

mac-address information enable (system view)

Syntax

mac-address information enable

undo mac-address information enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **mac-address information enable** command to enable MAC Information globally.

Use the **undo mac-address information enable** command to disable MAC Information globally.

By default, MAC Information is disabled globally.

Examples

Enable MAC Information globally.

```
<Sysname> system-view
[Sysname] mac-address information enable
```

mac-address information interval

Syntax

mac-address information interval *value*

undo mac-address information interval

View

System view

Default Level

2: System level

Parameters

value: Interval for sending Syslog or Trap messages (in seconds). The range for this argument is 1 to 20000.

Description

Use the **mac-address information interval** command to set the interval for sending Syslog or Trap messages.

Use the **undo mac-address information interval** command to restore the default interval for sending Syslog or Trap messages.

By default, the interval for sending Syslog or Trap messages is 1 second.

Examples

Set the interval for sending Syslog or Trap messages to 200 seconds.

```
<Sysname> system-view
[Sysname] mac-address information interval 200
```

mac-address information mode

Syntax

mac-address information mode { **syslog** | **trap** }

undo mac-address information mode

View

System view

Default Level

2: System level

Parameters

syslog: Specifies that the device sends Syslog messages to inform the remote network management device of MAC address changes.

trap: Specifies that the device sends trap messages to inform the remote network management device of MAC address changes.

Description

Use the **mac-address information mode** command to set the MAC Information mode, that is, whether to use Syslog messages or Trap messages to inform the remote network management device of MAC address changes.

Use the **undo mac-address information mode** command to restore the default.

By default, trap messages are sent to inform the remote network management device of MAC address changes.

Examples

Configure the device to send trap messages to inform the remote network management device of MAC address changes.

```
<Sysname> system-view
[Sysname] mac-address information mode trap
```

mac-address information queue-length

Syntax

mac-address information queue-length *value*

undo mac-address information queue-length

View

System view

Default Level

2: System level

Parameters

value: MAC Information queue length. The value range is 0 to 1000.

Description

Use the **mac-address information queue-length** command to set the MAC Information queue length.

Use the **undo mac-address information queue-length** command to restore the default.

By default, the MAC Information queue length is 50.

Setting the MAC Information queue length to 0 indicates that the device sends a Syslog or Trap message to the network management device as soon as a new MAC address is learned or an existing MAC address is deleted.

Examples

Set the MAC Information queue length to 600.

```
<Sysname> system-view
[Sysname] mac-address information queue-length 600
```

15 System Maintaining and Debugging Commands

System Maintaining Commands

ping

Syntax

ping [**ip**] [**-a** *source-ip* | **-c** *count* | **-f** | **-h** *ttl* | **-i** *interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-v** | **-vpn-instance** *vpn-instance-name*] * *remote-system*

View

Any view

Default Level

0: Visit level

Parameters

ip: Supports IPv4 protocol.

-a *source-ip*: Specifies the source IP address of an ICMP echo request (ECHO-REQUEST). It must be a legal IP address configured on the device.

-c *count*: Specifies the number of times that an ICMP echo request is sent, in the range 1 to 4294967295. The default value is 5.

-f: Discards packets larger than the MTU of a given interface, that is, the ICMP echo request is not allowed to be fragmented.

-h *ttl*: Specifies the TTL value for an ICMP echo request, in the range 1 to 255. The default value is 255.

-i *interface-type interface-number*: Specifies the ICMP echo request sending interface by its type and number.

-m *interval*: Specifies the interval (in milliseconds) to send an ICMP echo response, in the range 1 to 65535. The default value is 200 ms.

- If a response from the destination is received within the timeout time, the interval to send the next echo request equals the actual response period plus the value of *interval.*
- If no response from the destination is received within the timeout time, the interval to send the next echo request equals the *timeout* value plus the value of *interval.*

-n: Specifies that the Domain Name System (DNS) is disabled. DNS is enabled by default, that is, the *hostname* is translated into an address.

-p *pad*: Specifies the value of the **pad** field in an ICMP echo request, in hexadecimal format, 1 to 8 bits, in the range 0 to ffffffff. If the specified value is less than 8 bits, 0s will be added in front of the value to extend it to 8 bits. For example, if *pad* is configured as 0x2f, then the packets will be padded with 0x0000002f repeatedly to make the total length of the packet meet the requirements of the device. By

default, the padded value starts from 0x01 up to 0xff, where another round starts again if necessary, like 0x010203…feff01….

-q: Presence of this parameter indicates that only statistics are displayed. By default, all information is displayed.

-r: Records routes. By default, routes are not recorded.

-s *packet-size*: Specifies length (in bytes) of an ICMP echo request, in the range 20 to 8100. The default value is 56.

-t *timeout*: Specifies the timeout value (in milliseconds) of an ICMP echo reply (ECHO-REPLY), in the range 0 to 65535. It defaults to 2000.

-tos *tos*: Specifies type of service (ToS) of an echo request, in the range 0 to 255. The default value is 0.

-v: Displays non ICMP echo reply received. By default, the system does not display non ICMP echo reply.

-vpn-instance *vpn-instance-name*: Specifies the name of an MPLS VPN instance, which is a string of 1 to 31 characters. It is case sensitive.

remote-system: IP address or host name (a string of 1 to 20 characters) of the destination device.

Description

Use the **ping** command to verify whether the destination device in an IP network is reachable, and to display the related statistics.

Note that:

- You must use the command in the form of **ping ip** *ip* instead of **ping** *ip* if the destination name is a key word, such as **ip**.
- Only the directly connected segment address can be pinged if the outgoing interface is specified with the **-i** argument.

During the execution of the command, you can press **Ctrl+C** to abort the ping operation.

Examples

Check whether the device with an IP address of 10.1.1.5 is reachable.

```
<Sysname> ping 10.1.1.5
PING 10.1.1.5 : 56 data bytes, press CTRL_C to break
Reply from 10.1.1.5 : bytes=56 Sequence=1 ttl=255 time=1 ms
Reply from 10.1.1.5 : bytes=56 Sequence=2 ttl=255 time=2 ms
Reply from 10.1.1.5 : bytes=56 Sequence=3 ttl=255 time=1 ms
Reply from 10.1.1.5 : bytes=56 Sequence=4 ttl=255 time=3 ms
Reply from 10.1.1.5 : bytes=56 Sequence=5 ttl=255 time=2 ms

--- 10.1.1.5 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/2/3 ms
```

The above information indicates the following:

- The destination host was reachable

- All probe packets sent by the source device got responses
- The minimum time, average time, and maximum time for the packet's roundtrip time are 1 ms, 2 ms, and 3 ms respectively

Check whether the device with an IP address of 3.3.3.2 is reachable. Only the check results are displayed.

```
<Sysname> ping -q 3.3.3.2
  PING 3.3.3.2: 56  data bytes, press CTRL_C to break

  --- 3.3.3.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 1/1/1 ms
```

Check whether the device with an IP address of 3.3.3.2 is reachable. The route information is required to be displayed.

```
<Sysname> ping -r 3.3.3.2
  PING 3.3.3.2: 56  data bytes, press CTRL_C to break
    Reply from 3.3.3.2: bytes=56 Sequence=1 ttl=255 time=2 ms
      Record Route:
        3.3.3.2
        3.3.3.1
    Reply from 3.3.3.2: bytes=56 Sequence=2 ttl=255 time=1 ms
      Record Route:
        3.3.3.2
        3.3.3.1
    Reply from 3.3.3.2: bytes=56 Sequence=3 ttl=255 time=1 ms
      Record Route:
        3.3.3.2
        3.3.3.1
    Reply from 3.3.3.2: bytes=56 Sequence=4 ttl=255 time=2 ms
      Record Route:
        3.3.3.2
        3.3.3.1
    Reply from 3.3.3.2: bytes=56 Sequence=5 ttl=255 time=1 ms
      Record Route:
        3.3.3.2
        3.3.3.1

  --- 3.3.3.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 1/1/2 ms
```

The above information indicates the following:

- The destination host was reachable
- The IP address 3.3.3.1 was reached first, and then 3.3.3.2.

Table 15-1 ping command output description

Field	Description
PING 10.1.1.5	Check whether the device with IP address 10.1.1.5 is reachable
56 data bytes	Number of data bytes in the ICMP echo request
press CTRL_C to break	During the execution of the command, you can press **Ctrl+C** to abort the ping operation.
Reply from 10.1.1.5 : bytes=56 Sequence=1 ttl=255 time=1 ms	Received the ICMP reply from the device whose IP address is 10.1.1.5. If no reply is received during the timeout period, "Request time out" will be displayed. • bytes= indicates the number of data bytes in the ICMP reply. • Sequence= indicates the packet sequence. • ttl= indicates the TTL value in the ICMP reply. • time= indicates the response time.
Record Route:	The routers through which the ICMP echo request passed. They are displayed in inversed order, that is, the router with a smaller distance to the destination is displayed first.
--- 10.1.1.5 ping statistics ---	Statistics on data received and sent in the ping operation
5 packet(s) transmitted	Number of ICMP echo requests sent
5 packet(s) received	Number of ICMP echo requests received
0.00% packet loss	Percentage of packets not responded to the total packets sent
round-trip min/avg/max = 0/4/20 ms	Minimum/average/maximum response time, in ms

ping ipv6

Syntax

ping ipv6 [**-a** *source-ipv6* | **-c** *count* | **-m** *interval* | **-s** *packet-size* | **-t** *timeout*] * *remote-system* [**-i** *interface-type interface-number*]

View

Any view

Default Level

0: Visit level

Parameters

-a *source-ipv6*: Specifies the source IPv6 address of an ICMP echo request. It must be a legal IPv6 address configured on the device.

-c *count*: Specifies the number of times that an ICMPv6 echo request is sent, in the range 1 to 4294967295. The default value is 5.

-m *interval*: Specifies the interval (in milliseconds) to send an ICMPv6 echo reply, in the range 1 to 65535. The default value is 200 ms.

- If a response from the destination is received within the timeout time, the interval to send the next echo request equals the actual response period plus the value of *interval.*

- If no response from the destination is received within the timeout time, the interval to send the next echo request equals the *timeout* value plus the value of *interval.*

-s *packet-size*: Specifies length (in bytes) of an ICMPv6 echo request, in the range 20 to 8100. It defaults to 56.

-t *timeout*: Specifies the timeout value (in milliseconds) of an ICMPv6 echo reply, in the range 0 to 65535. It defaults to 2000.

remote-system: IPv6 address or host name of the destination device, a string of 1 to 46 characters.

-i *interface-type interface-number*: Specifies an outgoing interface by its type and number. This parameter can be used only in case that the destination address is the link local address and the specified outgoing interface must have a link local address (For the configuration of link local address, see *IPv6 Basics* in the *IP Services Volume*).

Description

Use the **ping ipv6** command to verify whether an IPv6 address is reachable, and display the corresponding statistics.

You must use the command in the form of **ping ipv6** *ipv6* instead of **ping** *ipv6* if the destination name is an ipv6 name.

During the execution of the command, you can press **Ctrl+C** to abort the ping ipv6 operation.

Examples

Verify whether the IPv6 address 2001::1 is reachable.

```
<Sysname> ping ipv6 2001::1
  PING 1::2 : 56  data bytes, press CTRL_C to break
    Reply from 1::2
    bytes=56 Sequence=1 hop limit=64  time = 4 ms
    Reply from 1::2
    bytes=56 Sequence=2 hop limit=64  time = 2 ms
    Reply from 1::2
    bytes=56 Sequence=3 hop limit=64  time = 2 ms
    Reply from 1::2
    bytes=56 Sequence=4 hop limit=64  time = 2 ms
    Reply from 1::2
    bytes=56 Sequence=5 hop limit=64  time = 2 ms

  --- 1::2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/4 ms
```

The “hop limit” field in this prompt information has the same meaning as the “ttl” field in the prompt information displayed by the IPv4 **ping** command, indicating the TTL value in the ICMPv6 echo request. For the description on other fields, refer to Table 15-1.

tracert

Syntax

tracert [**-a** *source-ip* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * *remote-system*

View

Any view

Default Level

0: Visit level

Parameters

-a *source-ip*: Specifies the source IP address of a tracert packet. It must be a legal IP address configured on the device.

-f *first-ttl*: Specifies the first TTL, that is, the allowed number of hops for the first packet, in the range 1 to 255. It defaults to 1 and must be less than the maximum TTL.

-m *max-ttl*: Specifies the maximum TTL, that is, the maximum allowed number of hops for a packet, in the range 1 to 255. It defaults to 30, and must be greater than the first TTL.

-p *port*: Specifies the UDP port number of the destination device, in the range 1 to 65535. The default value is 33434. You do not need to modify this parameter.

-q *packet-number*: Specifies the number of probe packets sent each time, in the range 1 to 65535. The default value is 3.

-vpn-instance *vpn-instance-name*: Specifies the name of an MPLS VPN instance, which is a string of 1 to 31 characters.

-w *timeout*: Specifies the timeout time of the reply packet of a probe packet, in the range 1 to 65535, in milliseconds. The default value is 5000 ms.

remote-system: IP address or host name (a string of 1 to 20 characters) of the destination device.

Description

Use the **tracert** command to trace the path the packets traverse from the source to the destination device.

After having identified network failure with the **ping** command, you can use the **tracert** command to determine the failed node(s).

Output information of the **tracert** command includes IP addresses of all the Layer 3 devices the packets traverse from the source to the destination device. If a device times out, "* * *" will be displayed.

During the execution of the command, you can press **Ctrl+C** to abort the tracert operation.

Examples

Display the path the packets traverse from the source device to the destination device with an IP address of 18.26.0.115.

```
<Sysname> tracert 18.26.0.115
traceroute to 18.26.0.115(18.26.0.115) 30 hops max,40 bytes packet, press CTRL_C to break
1  128.3.112.1  10 ms 10 ms 10 ms
```

```
2  128.32.210.1  19 ms 19 ms 19 ms
3  128.32.216.1  39 ms 19 ms 19 ms
4  128.32.136.23  19 ms 39 ms 39 ms
5  128.32.168.22  20 ms 39 ms 39 ms
6  128.32.197.4  59 ms 119 ms 39 ms
7  131.119.2.5  59 ms 59 ms 39 ms
8  129.140.70.13  80 ms 79 ms 99 ms
9  129.140.71.6  139 ms 139 ms 159 ms
10  129.140.81.7  199 ms 180 ms 300 ms
11  129.140.72.17  300 ms 239 ms 239 ms
12  * * *
13  128.121.54.72  259 ms 499 ms 279 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  18.26.0.115  339 ms 279 ms 279 ms
```

Table 15-2 tracert command output description

Field	Description
traceroute to 18.26.0.115(18.26.0.115)	Display the route the IP packets traverse from the current device to the device whose IP address is 18.26.0.115.
30 hops max	Maximum number of hops of the probe packets, which can be set through the **-m** keyword
60 bytes packet	Number of bytes of a probe packet
press CTRL_C to break	During the execution of the command, you can press **Ctrl+C** to abort the tracert operation.
1 128.3.112.1 10 ms 10 ms 10 ms	The probe result of the probe packets whose TTL is 1, including the IP address of the device and the roundtrip time of three probe packets. The number of packets that can be sent in each probe can be set through the **-q** keyword.
12 * * *	The probe result of the probe packets whose TTL is 12. The result is: timeout

tracert ipv6

Syntax

tracert ipv6 [**-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-w** *timeout*] * *remote-system*

View

Any view

Default Level

0: Visit level

Parameters

-f *first-ttl*: Specifies the first TTL, that is, the allowed number of hops for the first packet, in the range 1 to 255. It defaults to 1 and must be less than the maximum TTL.

-m *max-ttl*: Specifies the maximum TTL, that is, the maximum allowed number of hops for a packet, in the range 1 to 255. It defaults to 30 and must be greater than the first TTL.

-p *port*: Specifies the UDP port number of the destination device, in the range 1 to 65535. The default value is 33434. It is unnecessary to modify this parameter.

-q *packet-number*: Specifies the number of probe packets sent each time, in the range 1 to 65535, defaulting to 3.

-w *timeout*: Specifies the timeout time of the reply packet of a probe packet, in the range 1 to 65535, in milliseconds. The default value is 5000 ms.

remote-system: IPv6 address or host name of the destination device, a string of 1 to 46 characters.

Description

Use the **tracert ipv6** command to view the path the IPv6 packets traverse from the source to the destination device.

After having identified network failure with the **ping** command, you can use the **tracert** command to determine the failed node(s).

Output information of the **tracert ipv6** command includes IPv6 addresses of all the Layer 3 devices the packets traverse from the source to the destination device. If a device times out, "* * *" will be displayed.

During the execution of the command, you can press **Ctrl+C** to abort the tracert operation.

Examples

View the path the packets traverse from the source to the destination with IPv6 address 3002::1.

```
<Sysname> tracert ipv6 3002::1
 traceroute to 3002::1  30 hops max,60 bytes packet, press CTRL_C to break
 1 3003::1 30 ms 10 ms 10 ms
 2 3002::1 10 ms 11 ms 9 ms
```

For description on the fields in the above output information, refer to Table 15-2.

System Debugging Commands

debugging

Syntax

debugging { **all** [**timeout** *time*] | *module-name* [*option*] }

undo debugging { **all** | *module-name* [*option*] }

View

User view

Default Level

1: Monitor level

Parameters

all: All debugging functions.

timeout *time*: Specifies the timeout time for the **debugging all** command. When all debugging is enabled, the system automatically executes the **undo debugging all** command after the *time.* The value ranges from 1 to 1440, in minutes.

module-name: Module name, such as arp or device. You can use the **debugging ?** command to display the current module name.

option: The debugging option for a specific module. Different modules have different debugging options in terms of their number and content. You can use the **debugging** *module-name* **?** command to display the currently supported options.

Description

Use the **debugging** command to enable the debugging of a specific module.

Use the **undo debugging** command to disable the debugging of a specific module.

By default, debugging functions of all modules are disabled.

Note the following:

- Output of the debugging information may degrade system efficiency, so you are recommended to enable the debugging of a specific module for diagnosing network failure, and not to enable the debugging of multiple modules at the same time.
- **Default Level** describes the default level of the **debugging all** command. Different **debugging** commands may have different default levels.
- You must configure the **debugging**, **terminal debugging** and **terminal monitor** commands first to display detailed debugging information on the terminal. For the detailed description on the **terminal debugging** and **terminal monitor** commands, refer to *Information Center Commands* in the *System Volume*.

Related commands: **display debugging**.

Examples

Enable IP packet debugging.

```
<Sysname> debugging ip packet
```

display debugging

Syntax

display debugging [**interface** *interface-type interface-number*] [*module-name*]

View

Any view

Default Level

1: Monitor level

Parameters

interface *interface-type interface-number*: Displays the debugging settings of the specified interface, where *interface-type interface-number* represents the interface type and number.

module-name: Module name.

Description

Use the **display debugging** command to display enabled debugging functions.

Related commands: **debugging**.

Examples

Display all enabled debugging functions.

```
<Sysname> display debugging
IP packet debugging is on
```

16 Information Center Configuration Commands

Information Center Configuration Commands

display channel

Syntax

display channel [*channel-number* | *channel-name*]

View

Any view

Default Level

1: Monitor level

Parameters

channel-number: Displays information of the channel with a specified number, where *channel-number* represents the channel number, in the range 0 to 9.

channel-name: Displays information of the channel with a specified name, where *channel-name* represents the channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

Table 16-1 Information channels for different output destinations

Output destination	Information channel number	Default channel name
Console	0	console
Monitor terminal	1	monitor
Log host	2	loghost
Trap buffer	3	trapbuffer
Log buffer	4	logbuffer
SNMP module	5	snmpagent

Description

Use the **display channel** command to display channel information.

If no channel is specified, information for all channels is displayed.

Examples

Display information for channel 0.

```
<Sysname> display channel 0
```

```
channel number:0, channel name:console
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warnings      Y      debugging     Y      debugging
```

The above information indicates to output log information with the severity from 0 to 4, trap information with the severity from 0 to 7 and debugging information with the severity from 0 to 7 to the console. The information source modules are all modules (default).

Table 16-2 display channel command output description

Field	Description
channel number	A specified channel number, in the range 0 to 9.
channel name	A specified channel name, which varies with user's configuration. For more information, refer to the **info-center channel name** command.
MODU_ID	The ID of the module to which the information permitted to pass through the current channel belongs
NAME	The name of the module to which the information permitted to pass through the current channel belongs Default means all modules are allowed to output system information, but the module type varies with devices.
ENABLE	Indicates whether to enable or disable the output of log information, which could be Y or N.
LOG_LEVEL	The severity of log information, refer to Table 16-4 for details.
ENABLE	Indicates whether to enable or disable the output of trap information, which could be Y or N.
TRAP_LEVEL	The severity of trap information, refer to Table 16-4 for details.
ENABLE	Indicates whether to enable or disable the output of debugging information, which could be Y or N.
DEBUG_LEVEL	The severity of debugging information, refer to Table 16-4 for details.

display info-center

Syntax

display info-center

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display info-center** command to display the information of each output destination.

Examples

Display configurations on each output destination.

```
<Sysname> display info-center
Information Center:enabled
Log host:
   2.2.2.2, channel number : 8, channel name : channel8,
   host facility local7
Console:
   channel number : 0, channel name : console
Monitor:
   channel number : 1, channel name : monitor
SNMP Agent:
   channel number : 5, channel name : snmpagent
Log buffer:
   enabled,max buffer size 1024, current buffer size 512,
   current messages 512, dropped messages 0, overwritten messages 740
   channel number : 4, channel name : logbuffer
Trap buffer:
   enabled,max buffer size 1024, current buffer size 256,
   current messages 216, dropped messages 0, overwritten messages 0
   channel number : 3, channel name : trapbuffer
Information timestamp setting:
   log - date, trap - date, debug - date,
   loghost - date
```

Table 16-3 display info-center command output description

Field	Description
Information Center	The current state of the information center, which could be enabled or disabled.
Log host: 2.2.2.2, channel number : 8, channel name : channel8, host facility local7	Configurations on the log host destination (It can be displayed only when the **info-center loghost** command is configured), including IP address of the log host, the channel number and channel name used, and logging facility used.)
Console: channel number : 0, channel name : console	Configurations on the console destination, including the channel number and channel name used
Monitor: channel number : 1, channel name : monitor	Configurations on the monitor terminal destination, including the channel number and channel name used
SNMP Agent: channel number : 5, channel name : snmpagent	Configurations on the SNMP module destination, including the channel number and channel name used

Field	Description
Log buffer: enabled,max buffer size 1024, current buffer size 512, current messages 512, dropped messages 0, overwritten messages 740 channel number : 4, channel name : logbuffer	Configurations on the log buffer destination, including whether information output to this destination is enabled or disabled, the maximum capacity, the current capacity, the current number of messages, the number of dropped messages, the number of messages that have been overwritten, and the channel number and channel name used.
Trap buffer: enabled,max buffer size 1024, current buffer size 256, current messages 216, dropped messages 0, overwritten messages 0 channel number : 3, channel name : trapbuffer	Configurations on the trap buffer destination, including whether information output to this destination is enabled or disabled, the maximum capacity, the current capacity, the current number of messages, the number of dropped messages, the number of messages that have been overwritten, and the channel number and channel name used.
Information timestamp setting	The timestamp configurations, specifying the timestamp format for log, trap, debug, and log host information.

display logbuffer

Syntax

display logbuffer [**reverse**] [**level** *severity* | **size** *buffersize* | **slot** *slot-number*] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

reverse: Displays log entries chronologically, with the most recent entry at the top. If this keyword is not specified, the log entries will be displayed chronologically, with the oldest entry at the top.

level *severity*: Displays information of the log with specified level, where *severity* represents information level, in the range 0 to 7.

Table 16-4 Severity description

Severity	Value	Description
Emergency	0	The system is unusable.
Alert	1	Action must be taken immediately
Critical	2	Critical conditions
Error	3	Error conditions
Warning	4	Warning conditions
Notice	5	Normal but significant condition

Severity	Value	Description
Informational	6	Informational messages
Debug	7	Debug-level messages

size *buffersize*: Displays specified number of the latest log messages in the log buffer, where *buffersize* represents the number of the latest log messages to be displayed in the log buffer, in the range 1 to 1,024.

slot *slot-number*: Displays the log information in the log buffer of the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

|: Uses a regular expression to filter the output information. For detailed information about regular expression, refer to section CLI Display in *Basic System Configuration* in the *System Volume*.

- **begin**: Displays the line that matches the regular expression and all the subsequent lines.
- **exclude**: Displays the lines that do not match the regular expression.
- **include**: Displays the lines that match the regular expression.

regular-expression: Regular expression, a string of 1 to 256 characters. Note that this argument is case-sensitive and can have spaces included.

Description

Use the **display logbuffer** command to display the state of the log buffer and the log information recorded. Absence of the **size** *buffersize* argument indicates that all log information recorded in the log buffer is displayed.

Examples

Display the state of the log buffer and the log information recorded on the device.

```
<Sysname> display logbuffer
Logging buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 718
Current messages : 512

%Jun 17 15:57:09:578 2006 Sysname IC/7/SYS_RESTART:
System restarted --
```

The rest is omitted here.

Table 16-5 display logbuffer command output description

Field	Description
Logging buffer configuration and contents	Indicates the current state of the log buffer and its contents, which could be enabled or disabled.
Allowed max buffer size	The maximum buffer size allowed
Actual buffer size	The actual buffer size

Field	Description
Channel number	The channel number of the log buffer, defaults to 4.
Channel name	The channel name of the log buffer, defaults to logbuffer.
Dropped messages	The number of dropped messages
Overwritten messages	The number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	The number of the current messages

display logbuffer summary

Syntax

display logbuffer summary [**level** *severity* | **slot** *slot-number*] *

View

Any view

Default Level

1: Monitor level

Parameters

level *severity*: Displays the summary of the log buffer, where *severity* represents information level, in the range 0 to 7.

slot *slot-number*: Displays the summary of the log buffer of the specified device. If the device is in an IRF, the *slot-number* argument represents the member ID of the device; if the device is not in any IRF, the *slot-number* argument represents the device ID.

Description

Use the **display logbuffer summary** command to display the summary of the log buffer.

Examples

Display the summary of the log buffer on the device.

```
<Sysname> display logbuffer summary
  SLOT EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
     0     0     0     0     0     0     0     0     0
     1     0     0     0     0     0     0     0     0
     2     0     0     0     0     0     0     0     0
     3     0     0     0     0    16     0     1     0
```

Table 16-6 display logbuffer summary command output description

Field	Description
SLOT	Slot number

Field	Description
EMERG	Represents emergency, refer to Table 16-4 for details
ALERT	Represents alert, refer to Table 16-4 for details
CRIT	Represents critical, refer to Table 16-4 for details
ERROR	Represents error, refer to Table 16-4 for details
WARN	Represents warning, refer to Table 16-4 for details
NOTIF	Represents notice, refer to Table 16-4 for details
INFO	Represents informational, refer to Table 16-4 for details
DEBUG	Represents debug, refer to Table 16-4 for details

display trapbuffer

Syntax

display trapbuffer [**reverse**] [**size** *buffersize*]

View

Any view

Default Level

1: Monitor level

Parameters

reverse: Displays trap entries chronologically, with the most recent entry at the top. If this keyword is not specified, trap entries will be displayed chronologically, with the oldest entry at the top.

size *buffersize*: Displays specified number of the latest trap messages in a trap buffer, where *buffersize* represents the number of the latest trap messages in a trap buffer, in the range 1 to 1,024.

Description

Use the **display trapbuffer** command to display the state and the trap information recorded.

Absence of the **size** *buffersize* argument indicates that all trap information is displayed.

Examples

Display the state of the trap buffer and the trap information recorded.

```
<Sysname> display trapbuffer
Trapping buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 2

#Aug  7 14:47:35:636 2008 Sysname IFNET/4/INTERFACE UPDOWN:
```

```
 Trap 1.3.6.1.6.3.1.1.5.3<linkDown>: Interface 983041 is Down, ifAdminStatus is 2,
ifOperStatus is 2
#Aug  7 14:47:47:724 2008 Sysname IFNET/4/INTERFACE UPDOWN:
 Trap 1.3.6.1.6.3.1.1.5.4<linkUp>: Interface 983041 is Up, ifAdminStatus is 1, ifOperStatus
is 1
```

Table 16-7 display trapbuffer command output description

Field	Description
Trapping buffer configuration and contents	Indicates the current state of the trap buffer and its contents, which could be enabled or disabled.
Allowed max buffer size	The maximum buffer size allowed
Actual buffer size	The actual buffer size
Channel number	The channel number of the trap buffer, defaults to 3.
channel name	The channel name of the trap buffer, defaults to trapbuffer.
Dropped messages	The number of dropped messages
Overwritten messages	The number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	The number of the current messages

enable log updown

Syntax

enable log updown

undo enable log updown

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **enable log updown** command to allow a port to generate link up/down logging information when the port state changes.

Use the **undo enable log updown** command to disable a port from generating link up/down logging information when the port state changes.

By default, all the ports are allowed to generate port link up/down logging information when the port state changes.

Examples

Disable port GigabitEthernet 1/0/1 from generating link up/down logging information.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo enable log updown
```

info-center channel name

Syntax

info-center channel *channel-number* **name** *channel-name*

undo info-center channel *channel-number*

View

System view

Default Level

2: System level

Parameters

channel-number: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, a string of 1 to 30 characters. It must be a combination of letters and numbers, and start with a letter and is case insensitive.

Description

Use the **info-center channel name** command to name a channel with a specified channel number.

Use the **undo info-center channel** command to restore the default name for a channel with a specified channel number.

Refer to Table 16-1 for details of default channel names and channel numbers.

Examples

Name channel 0 as **abc**.

```
<Sysname> system-view
[Sysname] info-center channel 0 name abc
```

info-center console channel

Syntax

info-center console channel { *channel-number* | *channel-name* }

undo info-center console channel

View

System view

Default Level

2: System level

Parameters

channel-number: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

Description

Use the **info-center console channel** command to specify the channel to output system information to the console.

Use the **undo info-center console channel** command to restore the default output channel to the console.

By default, output of information to the console is enabled with channel 0 as the default channel (known as console).

Note that the **info-center console channel** command takes effect only after the information center is enabled first with the **info-center enable** command.

Examples

Set channel 0 to output system information to the console.

```
<Sysname> system-view
[Sysname] info-center console channel 0
```

info-center enable

Syntax

info-center enable

undo info-center enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **info-center enable** command to enable information center.

Use the **undo info-center enable** command to disable the information center.

The system outputs information to the log host or the console only after the information center is enabled first.

By default, the information center is enabled.

Examples

Enable the information center.

```
<Sysname> system-view
[Sysname] info-center enable
% Information center is enabled
```

info-center logbuffer

Syntax

info-center logbuffer [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *

undo info-center logbuffer [**channel** | **size**]

View

System view

Default Level

2: System level

Parameters

channel-number: A specified channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

buffersize: Specifies the maximum number of log messages that can be stored in a log buffer, in the range 0 to 1,024 with 512 as the default value.

Description

Use the **info-center logbuffer** command to enable information output to a log buffer and set the corresponding parameters.

Use the **undo info-center logbuffer** command to disable information output to a log buffer.

By default, information is output to the log buffer with the default channel of channel 4 (logbuffer) and the default buffer size of 512.

Note that the **info-center logbuffer** command takes effect only after the information center is enabled with the **info-center enable** command.

Examples

Configure the system to output information to the log buffer through channel 4, and set the log buffer size to 50.

```
<Sysname> system-view
[Sysname] info-center logbuffer size 50
```

info-center loghost

Syntax

info-center loghost *host-ip* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number*] *

undo info-center loghost *host-ip*

View

System view

Default Level

2: System level

Parameters

host-ip: The IP address of the log host.

channel: Specifies the channel through which system information can be output to the log host.

channel-number: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

facility *local-number*: The logging facility of the log host. The value can be local0 to local7 and defaults to local7. Logging facility is mainly used to mark different logging sources, query and filer the logs of the corresponding log source.

Description

Use the **info-center loghost** command to specify a log host and to configure the related parameters.

Use the **undo info-center loghost** command to restore the default configurations on a log host.

By default, output of system information to the log host is disabled. When it is enabled, the default channel name will be loghost and the default channel number will be 2.

Note that:

- The **info-center loghost** command takes effect only after the information center is enabled with the **info-center enable** command.
- Ensure to input a correct IP address while using the **info-center loghost** command to configure the IP address for a log host. System will prompt an invalid address if the loopback address (127.0.0.1) is input.
- A maximum number of 4 hosts (different) can be designated as the log host.

Examples

Output log information to a Unix station with the IP address being 1.1.1.1/16.

```
<Sysname> system-view
[Sysname] info-center loghost 1.1.1.1
```

info-center loghost source

Syntax

info-center loghost source *interface-type interface-number*

undo info-center loghost source

View

System view

Default Level

2: System level

Parameters

interface-type interface-number: Specifies the egress interface for log information by the interface type and interface number.

Description

Use the **info-center loghost source** command to specify the source IP address for log information.

Use the **undo info-center loghost source** command to restore the default.

By default, the interface for sending log information is determined by the matched route, and the primary IP address of this interface is the source IP address of the log information.

After the source IP address of log information is specified, no matter the log information is actually output through which physical interface, the source IP address of the log information is the primary IP address of the specified interface. If you want to display the source IP address in the log information, you can configure it by using this command.

Note that:

- The **info-center loghost source** command takes effect only after the information center is enabled with the **info-center enable** command.
- The IP address of the specified source interface must be configured; otherwise, although the **info-center loghost source** command can be configured successfully, the log host will not receive any log information.

Examples

By default, the log information in the following format is displayed on the log host:

```
<188>Jul 22 05:58:06 2008 Sysname %%10IFNET/4/LINK UPDOWN(l):  Vlan-interace1: link status is UP
```

Specify the primary IP address of VLAN-interace1 as the source IP address of log information.

```
<Sysname> system-view
[Sysname] interface Vlan-interace1
[Sysname-Vlan-interace1] ip address 2.2.2.2
[Sysname-Vlan-interace1] quit
[Sysname] info-center loghost source Vlan-interace1
```

After the above configuration, the log information in the following format is displayed on the log host (compared with the default format, the following format has the **-DevIP=2.2.2.2** field):

```
<188>Jul  22  06:11:31  2008  Sysname  %%10IFNET/4/LINK  UPDOWN(l):-DevIP=2.2.2.2; Vlan-interace1: link status is UP0
```

info-center monitor channel

Syntax

info-center monitor channel { *channel-number* | *channel-name* }

undo info-center monitor channel

View

System view

Default Level

2: System level

Parameters

channel-number: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

Description

Use the **info-center monitor channel** command to configure the channel to output system information to the monitor.

Use the **undo info-center monitor channel** command to restore the default channel to output system information to the monitor.

By default, output of system information to the monitor is enabled with a default channel name of monitor and a default channel number of 1.

Note that the **info-center monitor channel** command takes effect only after the information center is enabled with the **info-center enable** command.

Examples

Output system information to the monitor through channel 0.

```
<Sysname> system-view
[Sysname] info-center monitor channel 0
```

info-center snmp channel

Syntax

info-center snmp channel { *channel-number* | *channel-name* }

undo info-center snmp channel

View

System view

Default Level

2: System level

Parameters

channel-number: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

Description

Use the **info-center snmp channel** command to configure the channel to output system information to the SNMP module.

Use the **undo info-center snmp channel** command to restore the default channel to output system information to the SNMP module.

By default, output of system information to the SNMP module is enabled with a default channel name of snmpagent and a default channel number of 5.

For more information, refer to the **display snmp-agent** command in the *SNMP Commands* in the *System Volume*.

Examples

Output system information to the SNMP module through channel 6.

```
<Sysname> system-view
[Sysname] info-center snmp channel 6
```

info-center source

Syntax

info-center source { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**debug** { **level** *severity* | **state** *state* } * | **log** { **level** *severity* | **state** *state* } * | **trap** { **level** *severity* | **state** *state* } *] *

undo info-center source { *module-name* | **default** } **channel** { *channel-number* | *channel-name* }

View

System view

Default Level

2: System level

Parameters

module-name: Specifies the output rules of the system information of the specified modules. For instance, if information on ARP module is to be output, you can configure this argument as ARP. You can use the **info-center source ?** command to view the modules supported by the device.

default: Specifies the output rules of the system information of all the modules allowed to output the system information, including all the modules displayed by using the **info-center source ?** command.

debug: Debugging information.

log: Log information.

trap: Trap information.

level *severity*: Specifies the severity of system information, refer to Table 16-4 for details. With this keyword, you can specify the severity level of the information allowed/denied to output.

state *state*: Configures whether to output the system information, which could be **on** (enabled) or **off** (disabled). With this keyword, you can specify whether to output the specified system information.

channel-number: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

Description

Use the **info-center source** command to specify the output rules of the system information.

Use the **undo info-center source** command to remove the specified output rules.

By default, the output rules for the system information are listed in Table 16-8.

This command can be used to set the filter and redirection rules of log, trap and debugging information.

For example, the user can set to output log information with severity higher than warning to the log host, and information with severity higher than informational to the log buffer. The user can also set to output trap information of the IP module to a specified output destination.

Note that:

- If you do not use the *module-name* argument to set output rules for a module, the module uses the default output rules or the output rules set by the **default** keyword; otherwise the module uses the output rules separately set for it.
- If you use the default keyword to set the output rules for all the modules without specifying the **debug**, **log**, and **trap** keywords, the default output rules for the modules are used. Refer to Table 16-8 for details.
- If you use the *module-name* argument to set the output rules for a module without specifying the **debug**, **log**, and **trap** keywords, the default output rules for the module are as follows: the output of log and trap information is enabled, with severity being informational; the output of debugging information is disabled, with severity being debug. For example, if you execute the command **info-center source snmp channel** 5, the command is actually equal to the command **info-center source snmp channel 5 debug level debugging state off log level informational state on trap level informational state on**.
- If you repeatedly use the command to set the output rules for a module or for all the modules with the **default** keyword, the last configured output rules take effect
- After you separately set the output rules for a module, you must use the *module-name* argument to modify or remove the rules. The new configuration by using the **default** keyword is invalid on the module.
- You can configure to output the log, trap and debugging information to the trap buffer, but the trap buffer only receives the trap information and discards the log and debugging information.
- You can configure to output the log, trap and debugging information to the log buffer, but the log buffer only receives the log and debugging information and discards the trap information.
- You can configure to output the log, trap and debugging information to the SNMP module, but the SNMP module only receives the trap information and discards the log and debugging information.

Table 16-8 Default output rules for different output destinations

Output destination	Modules allowed	LOG		TRAP		DEBUG	
		Enabled/ disabled	Severity	Enabled/ disabled	Severity	Enabled/ disabled	Severity
Console	default (all modules)	Enabled	Warning	Enabled	Debug	Enabled	Debug

Output destination	Modules allowed	LOG		TRAP		DEBUG	
		Enabled/ disabled	Severity	Enabled/ disabled	Severity	Enabled/ disabled	Severity
Monitor terminal	default (all modules)	Enabled	Warning	Enabled	Debug	Enabled	Debug
Log host	default (all modules)	Enabled	Informational	Enabled	Debug	Disabled	Debug
Trap buffer	default (all modules)	Disabled	Informational	Enabled	Warning	Disabled	Debug
Log buffer	default (all modules)	Enabled	Warning	Disabled	Debug	Disabled	Debug
SNMP module	default (all modules)	Disabled	Debug	Enabled	Warning	Disabled	Debug

Examples

Set the output channel for the log information of VLAN module to **snmpagent** and to output information with severity being **emergency**. Log information of other modules cannot be output to this channel; other types of information of this module may or may not be output to this channel.

```
<Sysname> system-view
[Sysname] info-center source default channel snmpagent log state off
[Sysname] info-center source vlan channel snmpagent log level emergencies state on
```

Set the output channel for the log information of VLAN module to **snmpagent** and to output information with severity being **emergency**. Log information of other modules and all the other system information cannot be output to this channel.

```
<Sysname> system-view
[Sysname] info-center source default channel snmpagent debug state off log state off trap
state off
[Sysname] info-center source vlan channel snmpagent log level emergencies state on
```

info-center synchronous

Syntax

info-center synchronous

undo info-center synchronous

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **info-center synchronous** command to enable synchronous information output.

Use the **undo info-center synchronous** command to disable the synchronous information output.

By default, the synchronous information output is disabled.

Note

- If system information, such as log information, is output before you input any information under a current command line prompt, the system will not display the command line prompt after the system information output.
- If system information is output when you are inputting some interactive information (non Y/N confirmation information), then after the system information output, the system will not display the command line prompt but your previous input in a new line.

Examples

Enable the synchronous information output function, and then input the **display interface gigabitethe** command to view Ethernet interface information.

```
<Sysname> system-view
[Sysname] info-center synchronous
% Info-center synchronous output is on
[Sysname] display interface gigabitethe
```

At this time, the system receives log messages, and it then displays the log messages first. After the system displays all the log messages, it displays the user's previous input, which is **display interface gigabitethe** in this example.

```
%Apr 29 08:12:44:71 2007 Sysname IFNET/4/LINK UPDOWN:
 GigabitEthernet1/0/1: link status is UP
[Sysname] display interface gigabitethe
```

After the above information is displayed, you can input **rnet** to complete your input of the **display interface gigabitethernet** command, and then press the **Enter** key to execute the command.

Enable the synchronous information output function, and then save the current configuration (input interactive information).

```
<Sysname> system-view
[Sysname] info-center synchronous
% Info-center synchronous output is on
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:
```

At this time, the system receives the log information, and it then displays the log information first. After the system displays all the log information, it displays the user's previous input, which is [Y/N] in this example.

```
%May 21 14:33:19:425 2007 Sysname SHELL/4/LOGIN: VTY login from 192.168.1.44
[Y/N]:
```

After the above information is displayed, you can input **Y** or **N** to complete your input before the output of the log information.

info-center timestamp

Syntax

info-center timestamp { **debugging** | **log** | **trap** } { **boot** | **date** | **none** }

undo info-center timestamp { **debugging** | **log** | **trap** }

View

System view

Default Level

2: System level

Parameters

debugging: Sets the timestamp format of the debugging information.

log: Sets the timestamp output format of the log information.

trap: Sets the timestamp output format of the trap information.

boot: The time taken to boot up the system, in the format of xxxxxx.yyyyyy, in which xxxxxx represents the most significant 32 bits of the time taken to boot up the system (in milliseconds) whereas yyyyyy is the least significant 32 bits. For example, 0.21990989 equals Jun 25 14:09:26:881 2007.

date: The current system date and time, in the format of “Mmm dd hh:mm:ss:sss yyyy”.

- Mmm: The abbreviations of the months in English, which could be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
- dd: The date, starting with a space if less than 10, for example “ 7”.
- hh:mm:ss:sss: The local time, with hh ranging from 00 to 23, mm and ss ranging from 00 to 59, and sss ranging from 0 to 999.
- yyyy: Represents the year.

none: Indicates no time information is provided.

Description

Use the **info-center timestamp** command to configure the timestamp format.

Use the **undo info-center timestamp** command to restore the default.

By default, the timestamp format of log, trap and debugging information is **date**.

Examples

Configure the timestamp format for log information as **boot**.

```
<Sysname> system-view
[Sysname] info-center timestamp log boot
```

At this time, if you execute the **shutdown** command on GigabitEthernet1/0/1 that is in the UP state, the log information generated is as follows:

```
%0.1382605158 Sysname IFNET/4/LINK UPDOWN:
```

```
 GigabitEthernet1/0/1: link status is DOWN
```

Configure the timestamp format for log information as **date**.

```
<Sysname> system-view
[Sysname] info-center timestamp log date
```

At this time, if you execute the **shutdown** command on GigabitEthernet1/0/1 that is in the UP state, the log information generated is as follows:

```
%Sep 29 17:19:11:188 2007 Sysname IFNET/4/LINK UPDOWN:
 GigabitEthernet1/0/1: link status is DOWN
```

Configure the timestamp format for log information as **none**.

```
<Sysname> system-view
[Sysname] info-center timestamp log none
```

At this time, if you execute the **shutdown** command on GigabitEthernet1/0/1 that is in the UP state, the log information generated is as follows:

```
% Sysname IFNET/4/LINK UPDOWN:
 GigabitEthernet1/0/1: link status is DOWN
```

info-center timestamp loghost

Syntax

info-center timestamp loghost { **date** | **no-year-date** | **none** }

undo info-center timestamp loghost

View

System view

Default Level

2: System level

Parameters

date: Indicates the current system date and time, in the format of "Mmm dd hh:mm:ss:ms yyyy". However, the display format depends on the log host.

no-year-date: Indicates the current system date and time (year exclusive).

none: Indicates that no time stamp information is provided.

Description

Use the **info-center timestamp loghost** command to configure the time stamp format of the system information sent to the log host.

Use the **undo info-center timestamp loghost** command to restore the default.

By default, the time stamp format for system information sent to the log host is **date.**

Examples

Configure that the system information output to the log host does not include the year information.

```
<Sysname> system-view
[Sysname] info-center timestamp loghost no-year-date
```

info-center trapbuffer

Syntax

info-center trapbuffer [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *

undo info-center trapbuffer [**channel** | **size**]

View

System view

Default Level

2: System level

Parameters

size *buffersize*: Specifies the maximum number of trap messages in a trap buffer, in the range 0 to 1,024 with 256 as the default value.

channel-number: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or a self-defined name. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to the **info-center channel name** command.

Description

Use the **info-center trapbuffer** command to enable information output to the trap buffer and set the corresponding parameters.

Use the **undo info-center trapbuffer** command to disable information output to the trap buffer.

By default, information output to the trap buffer is enabled with channel 3 (trapbuffer) as the default channel and a maximum buffer size of 256.

Note that the **info-center trapbuffer** command takes effect only after the information center is enabled with the **info-center enable** command.

Examples

Configure the system to output information to the trap buffer through the default channel, and set the trap buffer size to 30.

```
<Sysname> system-view
[Sysname] info-center trapbuffer size 30
```

reset logbuffer

Syntax

reset logbuffer

View

User view

Default Level

3: Manage level

Parameters

None

Description

Use the **reset logbuffer** command to reset the log buffer contents.

Examples

Reset the log buffer contents.

```
<Sysname> reset logbuffer
```

reset trapbuffer

Syntax

reset trapbuffer

View

User view

Default Level

3: Manage level

Parameters

None

Description

Use the **reset trapbuffer** command to reset the trap buffer contents.

Examples

Reset the trap buffer contents.

```
<Sysname> reset trapbuffer
```

terminal debugging

Syntax

terminal debugging

undo terminal debugging

View

User view

Default Level

1: Monitor level

Parameters

None

Description

Use the **terminal debugging** command to enable the display of debugging information on the current terminal.

Use the **undo terminal debugging** command to disable the display of debugging information on the current terminal.

By default, the display of debugging information on the current terminal is disabled.

Note that:

- The debugging information is displayed (using the **terminal debugging** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).
- The configuration of this command is valid for only the current connection between the terminal and the device. If a new connection is established, the display of debugging information on the terminal restores the default.

Examples

Enable the display of debugging information on the current terminal.

```
<Sysname> terminal debugging
% Current terminal debugging is on
```

terminal logging

Syntax

terminal logging

undo terminal logging

View

User view

Default Level

1: Monitor level

Parameters

None

Description

Use the **terminal logging** command to enable the display of log information on the current terminal.

Use the **undo terminal logging** command to disable the display of log information on the current terminal.

By default, the display of log information on the current terminal is disabled.

Note that:

- The log information is displayed (using the **terminal logging** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).

- The configuration of this command is valid for only the current connection between the terminal and the device. If a new connection is established, the display of log information on the terminal restores the default.

Examples

Disable the display of log information on the current terminal.

```
<Sysname> undo terminal logging
% Current terminal logging is off
```

terminal monitor

Syntax

terminal monitor

undo terminal monitor

View

User view

Default Level

1: Monitor level

Parameters

None

Description

Use the **terminal monitor** command to enable the monitoring of system information on the current terminal.

Use the **undo terminal monitor** command to disable the monitoring of system information on the current terminal.

By default, monitoring of the system information on the console is enabled and that on the monitor terminal is disabled.

Note that:

- You need to configure the **terminal monitor** command before you can display the log, trap, and debugging information.
- Configuration of the **undo terminal monitor** command automatically disables the monitoring of log, trap, and debugging information.
- The configuration of this command is valid for only the current connection between the terminal and the device. If a new connection is established, the monitoring of system information on the terminal restores the default.

Examples

Enable the monitoring of system information on the current terminal.

```
<Sysname> terminal monitor
% Current terminal monitor is on
```

terminal trapping

Syntax

terminal trapping

undo terminal trapping

View

User view

Default Level

1: Monitor level

Parameters

None

Description

Use the **terminal trapping** command to enable the display of trap information on the current terminal.

Use the **undo terminal trapping** command to disable the display of trap information on the current terminal.

By default, the display of trap information on the current terminal is enabled.

Note that:

- The trap information is displayed (using the **terminal trapping** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).
- The configuration of this command is valid for only the current connection between the terminal and the device. If a new connection is established, the display of trap information on the terminal restores the default.

Examples

Enable the display of trap information on the current terminal.

```
<Sysname> terminal trapping
% Current terminal trapping is on
```

17 Hotfix Configuration Commands

Hotfix Configuration Commands

display patch information

Syntax

display patch information

View

Any view

Default Level

3: Manage level

Parameters

None

Description

Use the **display patch information** command to display the hotfix information.

Examples

Display hotfix information.

```
<Sysname> display patch information
The location of patches: flash:/
Slot Version   Temporaty Common Current Active Running  Start-Address
-------------------------------------------------------------------------
1    XXX002    0         1      1       0      0        0x4accf74
2    XXX       0         0      0       0      0        0x4accf74
```

Table 17-1 display patch information command output description

Field	Description
The location of patches	Patch file location. You can configure it using the **patch location** command.
Slot	Member ID
Version	Patch version. The first three characters represent the suffix of the PATCH-FLAG. For example, if the PATCH-FLAG of the a device is PATCH-RPE, "RPE" is displayed. The following three digits, if any, represent the patch number. (The patch number can be read after the patch is loaded.)
Temporary	Number of temporary patches
Common	Number of common patches

Field	Description
Current	Total number of patches
Running	Number of patches in the RUNNING state
Active	Number of patches in the ACTIVE state
Start-Address	Starting address of the memory patch area in the memory

patch active

Syntax

patch active *patch-number* **slot** *slot-number*

View

System view

Default Level

3: Manage level

Parameters

patch-number: Sequence number of a patch. The valid values of this argument depend on the patch file used.

slot *slot-number*: Specifies a member device by its member ID. The value range of this argument varies with the device model and can be displayed through the **display irf** command.

Description

Use the **patch active** command to activate the specified patch, namely, the system will run the patch.

After you execute the command, all the DEACTIVE patches before the specified patch number are activated.

Note that:

- The command is not applicable to patches in the DEACTIVE state.
- After a system reboot, the original ACTIVE patches change to DEACTIVE and become invalid. To make them effective, you need to activate them again.

Examples

Activate patch 3 and all the DEACTIVE patches before patch 3 on the device with member ID being 1.

```
<Sysname> system-view
[Sysname] patch active 3 slot 1
```

patch deactive

Syntax

patch deactive *patch-number* **slot** *slot-number*

View

System view

Default Level

3: Manage level

Parameters

patch-number: Sequence number of a patch. The valid values of this argument depend on the patch file used.

slot *slot-number*: Specifies a member device by its member ID. The value range of this argument varies with the device model and can be displayed through the **display irf** command.

Description

Use the **patch deactive** command to stop running the specified patch and all the ACTIVE patches before the specified patch number, and the system will run at the original software version.

All the ACTIVE patches (including the specified patch) turn to DEACTIVE state.

This command is not applicable to the patches in the RUNNING state.

Examples

Stop running patch 3 and all the ACTIVE patches before patch 3 on the device with member ID being 1.

```
<Sysname> system-view
[Sysname] patch deactive 3 slot 1
```

patch delete

Syntax

patch delete *patch-number* **slot** *slot-number*

View

System view

Default Level

3: Manage level

Parameters

patch-number: Sequence number of a patch. The valid values of this argument depend on the patch file used.

slot *slot-number*: Specifies a member device by its member ID. The value range of this argument varies with the device model and can be displayed through the **display irf** command.

Description

Use the **patch delete** command to delete the specified patch and all the patches before the specified patch number.

This command only removes the patches from the memory patch area, and it does not delete them from the storage medium. The patches are in the IDLE state after execution of this command.

Examples

Delete patch 3 and all the patches before patch 3 on the device with member ID being 1.

```
<Sysname> system-view
[Sysname] patch delete 3 slot 1
```

patch install

Syntax

patch install *patch-location*

undo patch install

View

System view

Default Level

3: Manage level

Parameters

patch-location: A string consisting of 1 to 64 characters. About the switch 4210G, the location is “flash:”.

Description

Use the **patch install** command to install all the patches in one step.

Use the **undo patch install** to remove the patches.

After you execute the **patch install** command, a message "Do you want to continue running patches after reboot? [Y/N]:" is displayed.

- Entering **y** or **Y**: All the specified patches are installed, and turn to the RUNNING state from IDLE. This equals execution of the commands **patch location**, **patch load**, **patch active**, and **patch run**. The patches remain RUNNING after system reboot.
- Entering **n** or **N**: All the specified patches are installed and turn to the ACTIVE state from IDLE. This equals execution of the commands **patch location**, **patch load** and **patch active**. The patches turn to the DEACTIVE state after system reboot.

Note that:

- Before executing the command, save the patch files to root directories of the member devices' storage media.
- The **patch install** command changes the patch file location specified with the **patch location** command to the directory specified by the *patch-file* argument of the **patch install** command. For example, if you execute the **patch location** *xxx* command and then the **patch install** *yyy* command, the patch file location automatically changes from xxx to yyy.

Examples

Install the patches located on the flash.

```
<Sysname> system-view
[Sysname] patch-install flash:
Patches will be installed. Continue? [Y/N]:y
Do you want to run patches after reboot? [Y/N]:y
```

```
Installing patches…
Installation completed, and patches will continue to run after reboot.
[Sysname]
```

patch load

Syntax

patch load slot *slot-number*

View

System view

Default Level

3: Manage level

Parameters

slot *slot-number*: Specifies a member device by its member ID. The value range of this argument varies with the device model and can be displayed through the **display irf** command.

Description

Use the **patch load** command to load the patch file on the storage medium.

Before using the command, save the patch files to the root directories of the member devices' storage media.

Examples

Load the patch files for the device with member ID being 1.

```
<Sysname> system-view
[Sysname] patch load slot 1
```

patch location

Syntax

patch location *patch-location*

View

System view

Default Level

3: Manage level

Parameters

patch-location: Specifies the patch file location. It is a string consisting of 1 to 64 characters. About the switch 4210G, the location is “flash:”.

Description

Use the **patch location** command to configure the patch file location.

By default, the patch file location is **flash:**.

Note that the **patch install** command changes the patch file location specified with the **patch location** command to the directory specified by the *patch-location* argument of the **patch install** command. For example, if you execute the **patch location** *xxx* command and then the **patch install** *yyy* command, the patch file location automatically changes from xxx to yyy.

Examples

Configure the root directory of the flash as the patch file location.

```
<Sysname> system-view
[Sysname] patch location flash:
```

patch run

Syntax

patch run *patch-number* [**slot** *slot-number*]

View

System view

Default Level

3: Manage level

Parameters

patch-number: Sequence number of a patch. The valid values of this argument depend on the patch file used.

slot *slot-number*: Specifies a member device by its member ID. The value range of this argument varies with the device model and can be displayed through the **display irf** command.

Description

Use the **patch run** command to confirm the running of the specified patch and all the ACTIVE patches before the specified patch number.

With the **slot** keyword specified, the command confirms the running state of all the qualified patches on a member device. If the keyword is not specified, the command confirms the running state of all the qualified patches on all the member devices.

This command is applicable to patches in the ACTIVE state only.

If the running of a patch is confirmed, after the system reboots, the patch will still be effective.

Examples

Confirm the running of patch 3 and all the ACTIVE patches before patch 3 on the device with member ID being 1.

```
<Sysname> system-view
[Sysname] patch run 3 slot 1
```

18 NQA Configuration Commands

NQA Client Configuration Commands

advantage-factor

Syntax

advantage-factor *factor*

undo advantage-factor

View

Voice test type view

Default Levels

2: System level

Parameter

factor: Advantage factor, used to count Mean Opinion Scores (MOS) and Calculated Planning Impairment Factor (ICPIF) values. It is in the range 0 to 20.

Description

Use the **advantage-factor** command to configure the advantage factor which is used to count MOS and ICPIF values.

Use the **undo advantage-factor** command to restore the default.

By default, the advantage factor is 0.

The evaluation of voice quality depends on users' tolerance to voice quality, and this factor should be taken into consideration. For users with higher tolerance to voice quality, you can use the **advantage-factor** command to configure the advantage factor. When the system calculates the ICPIF value, this advantage factor is subtracted to modify ICPIF and MOS values and thus both the objective and subjective factors are considered when you evaluate the voice quality.

Example

Configure the advantage factor for a voice test as 10.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] advantage-factor 10
```

codec-type

Syntax

codec-type { **g711a** | **g711u** | **g729a** }

undo codec-type

View

Voice test type view

Default Level

2: System level

Parameters

g711a: G.711 A-law codec type.

g711u: G.711 μ-law codec type

g729a: G.729 A-law codec type.

Description

Use the **codec-type** command to configure the codec type for a voice test.

Use the **undo codec-type** command to restore the default.

By default, the codec type for a voice test is G.711 A-law.

Examples

Configure the codec type for a voice test as **g729a**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type voice
[Sysname-nqa-admin-test-voice] codec-type g729a
```

data-fill

Syntax

data-fill *string*

undo data-fill

View

ICMP echo, UDP echo, UDP jitter, voice test type view

Default Level

2: System level

Parameters

string: String used to fill a probe packet, in the range 1 to 200. It is case sensitive.

Description

Use the **data-fill** command to configure the string used to fill a probe packet.

Use the **undo data-fill** command to restore the default.

By default, the string used to fill a probe packet is the hexadecimal number 00010203040506070809.

- If the data field of a probe packet is smaller than the fill data, the system uses only the first part of the character string to encapsulate the packet.
- If the data field of a probe packet is larger than the fill data, the system fills the character string cyclically to encapsulate the packet until it is full.

For example, when the fill data is **abcd** and the size of the data field of a probe packet is 3 byte, **abc** is used to fill the packet. When the data field of a probe packet is 6 byte, **abcdab** is used to fill the packet.

- In an ICMP echo test, the configured character string is used to fill the data field in an ICMP echo message.
- In a UDP echo test, because the first five bytes of the data field of a UDP packet have some specific usage, the configured character string is used to fill the remaining bytes in the UDP packet.
- In a UDP jitter test, because the first 68 bytes of the data field of a UDP packet have some specific usage, the configured character string is used to fill the remaining bytes in the UDP packet.
- In a voice test, because the first 16 bytes of the data field of a UDP packet have some specific usage, the configured character string is used to fill the remaining bytes in the UDP packet.

Examples

Configure the string used to fill an ICMP echo probe packet as **abcd**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-fill abcd
```

data-size

Syntax

data-size *size*

undo data-size

View

ICMP echo, UDP echo, UDP jitter, voice test type view

Default Level

2: System level

Parameters

size: Size of a probe packet in bytes, in the range 20 to 8100 for an ICMP echo or a UDP echo test, in the range 68 to 8100 for a UDP jitter test and in the range 16 to 1500 for a voice test.

Description

Use the **data-size** command to configure the size of a probe packet to be sent.

Use the **undo data-size** command to restore the default.

The default values are as shown in Table 18-1.

Table 18-1 Default values of the size of test packets sent

Test Type	Codec type	Default value (in bytes)
ICMP	None	100
UDP echo	None	100
UDP jitter	None	100
Voice	G.711 A-law	172
Voice	G.711 μ-law	172
Voice	G.729 A-law	32

- For an ICMP echo test, the size of a probe packet is the length of the data field in an ICMP echo message.
- For a UDP echo test, UDP jitter test and voice test, the size of a probe packet is the length of the data field in a UDP packet.

Examples

Configure the size of an ICMP echo probe packet as 80 bytes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-size 80
```

description (any NQA test type view)

Syntax

description *text*

undo description

View

Any NQA test type view

Default Level

2: System level

Parameters

text: Descriptive string of a test group, in the range 1 to 200. It is case sensitive.

Description

Use the **description** command to give a brief description of a test group, usually, the test type or test purpose of a test group.

Use the **undo description** command to remove the configured description information.

By default, no descriptive string is available for a test group.

Examples

Configure the descriptive string for a test group as **icmp-probe**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] description icmp-probe
```

destination ip

Syntax

destination ip *ip-address*

undo destination ip

View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default Level

2: System level

Parameters

ip-address: Destination IP address of a test operation.

Description

Use the **destination ip** command to configure a destination IP address for a test operation.

Use the **undo destination ip** command to remove the configured destination IP address.

By default, no destination IP address is configured for a test operation.

Examples

Configure the destination IP address of an ICMP echo test operation as 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
```

destination port

Syntax

destination port *port-number*

undo destination port

View

TCP, UDP echo, UDP jitter, voice test type view

Default Level

2: System level

Parameters

port-number: Destination port number of a test operation, in the range 1 to 65535.

Description

Use the **destination port** command to configure a destination port number for a test operation.

Use the **undo destination port** command to remove the configured destination port number.

By default, no destination port number is configured for a test operation.

Note that you are not recommended to perform a UDP jitter test and a voice test on ports from 1 to 1023 (known ports). Otherwise, the NQA test will fail or the corresponding services of this port will be unavailable.

Examples

Configure the destination port number of a test operation as 9000.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] destination port 9000
```

display nqa history

Syntax

display nqa history [*admin-name operation-tag*]

View

Any view

Default Level

2: System level

Parameters

admin-name operation-tag: Displays history records of a test group. If these two arguments are not specified, history records of all test groups are displayed. *admin-name* represents the name of the administrator who creates the NQA operation. It is a string of 1 to 32 characters, case-insensitive. *operation-tag* represents the test operation tag. It is a string of 1 to 32 characters, case-insensitive.

Description

Use the **display nqa history** command to display history records of NQA tests.

The **display nqa history** command cannot show you the results of voice tests and UDP jitter tests. Therefore, to know the result of a voice test or a UDP jitter test, you are recommended to use the **display nqa result** command to view the probe results of the latest NQA test, or use the **display nqa statistics** command to view the statistics of NQA tests.

Examples

Display the history records of the NQA test in which the administrator name is **administrator**, and the operation tag is **test**.

```
<Sysname> display nqa history administrator test
  NQA entry(admin administrator, tag test) history record(s):
    Index      Response     Status          Time
    10         329          Succeeded       2007-04-29 20:54:26.5
```

```
9           344         Succeeded       2007-04-29 20:54:26.2
8           328         Succeeded       2007-04-29 20:54:25.8
7           328         Succeeded       2007-04-29 20:54:25.5
6           328         Succeeded       2007-04-29 20:54:25.1
5           328         Succeeded       2007-04-29 20:54:24.8
4           328         Succeeded       2007-04-29 20:54:24.5
3           328         Succeeded       2007-04-29 20:54:24.1
2           328         Succeeded       2007-04-29 20:54:23.8
1           328         Succeeded       2007-04-29 20:54:23.4
```

Table 18-2 display nqa history command output description

Field	Description
Index	History record number
Response	Roundtrip delay of a test packet in the case of a successful test, timeout time in the case of timeout, or 0 in the case that a test cannot be completed (in milliseconds)
Status	Status value of test results, including: • Succeeded • Unknown error • Internal error • Timeout
Time	Time when the test is completed

display nqa result

Syntax

display nqa result [*admin-name operation-tag*]

View

Any view

Default Level

2: System level

Parameters

admin-name operation-tag: Displays results of the last test of a test group. If this argument is not specified, results of the last tests of all test groups are displayed. *admin-name* represents the name of the administrator who creates the NQA operation. It is a string of 1 to 32 characters, case-insensitive. *operation-tag* represents the test operation tag. It is a string of 1 to 32 characters, case-insensitive.

Description

Use the **display nqa result** command to display results of the last NQA test.

Examples

Display the results of the last UDP jitter test.

```
<Sysname> display nqa result admin test
```

```
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 192.168.1.42
      Send operation times: 10          Receive response times: 10
      Min/Max/Average round trip time: 15/46/26
      Square-Sum of round trip time: 8103
      Last succeeded probe time: 2008-05-29 10:56:38.7
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    UDP-jitter results:
     RTT number: 10
      Min positive SD: 8                Min positive DS: 8
      Max positive SD: 18               Max positive DS: 8
      Positive SD number: 5             Positive DS number: 2
      Positive SD sum: 75               Positive DS sum: 32
      Positive SD average: 15           Positive DS average: 16
      Positive SD square sum: 1189      Positive DS square sum: 640
      Min negative SD: 8                Min negative DS: 1
      Max negative SD: 24               Max negative DS: 30
      Negative SD number: 4             Negative DS number: 7
      Negative SD sum: 56               Negative DS sum: 99
      Negative SD average: 14           Negative DS average: 14
      Negative SD square sum: 946       Negative DS square sum: 1495
    One way results:
      Max SD delay: 22                  Max DS delay: 23
      Min SD delay: 7                   Min DS delay: 7
      Number of SD delay: 10            Number of DS delay: 10
      Sum of SD delay: 125              Sum of DS delay: 132
      Square sum of SD delay: 1805      Square sum of DS delay: 1988
      SD lost packet(s): 0              DS lost packet(s): 0
      Lost packet(s) for unknown reason: 0
```

Display the results of the last voice test.

```
<Sysname> display nqa result admin test
  NQA entry(admin admin, tag test) test results:
    Destination IP address: 192.168.1.42
      Send operation times: 1000        Receive response times: 0
      Min/Max/Average round trip time: 0/0/0
      Square-Sum of round trip time: 0
      Last succeeded probe time: 0-00-00 00:00:00.0
    Extended results:
      Packet lost in test: 100%
```

```
  Failures due to timeout: 1000
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to sequence error: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packet(s) arrived late: 0
Voice results:
 RTT number: 0
  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 average: 0            Positive DS average: 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 average: 0            Negative DS average: 0
  Negative SD square sum: 0         Negative DS square sum: 0
One way results:
  Max SD delay: 0                   Max DS delay: 0
  Min SD delay: 0                   Min DS delay: 0
  Number of SD delay: 0             Number of DS delay: 0
  Sum of SD delay: 0                Sum of DS delay: 0
  Square sum of SD delay: 0         Square sum of DS delay: 0
  SD lost packet(s): 0              DS lost packet(s): 0
  Lost packet(s) for unknown reason: 1000
Voice scores:
  MOS value: 0.99                   ICPIF value: 87
```

Table 18-3 display nqa result command output description

Field	Description
Destination IP address	IP address of the destination
Send operation times	Number of probe packets sent
Receive response times	Number of response packets received
Min/Max/Average round trip time	Minimum/maximum/average roundtrip time, in milliseconds
Square-Sum of round trip time	Square sum of roundtrip time
Last succeeded probe time	Time when the last successful probe was finished
Packet lost in test	Average packet loss ratio
Failures due to timeout	Number of timeout occurrences in a test
Failures due to disconnect	Number of disconnections by the peer
Failures due to no connection	Number of failures to connect with the peer

Field	Description
Failures due to sequence error	Number of failures owing to out-of-sequence packets
Failures due to internal error	Number of failures owing to internal errors
Failures due to other errors	Failures due to other errors
Packet(s) arrived late	Number of packets that arrived late
UDP-jitter results	UDP jitter test results, available only in UDP jitter tests.
Voice results	Voice test results, available only in voice tests.
RTT number	Number of response packets received
Min positive SD	Minimum positive jitter delay from source to destination
Min positive DS	Minimum positive jitter delay from destination to source
Max positive SD	Maximum positive jitter delay from source to destination
Max positive DS	Maximum positive jitter delay from destination to source
Positive SD number	Number of positive jitter delays from source to destination
Positive DS number	Number of positive jitter delays from destination to source
Positive SD sum	Sum of positive jitter delays from source to destination
Positive DS sum	Sum of positive jitter delays from destination to source
Positive SD average	Average of positive jitter delays from source to destination
Positive DS average	Average of positive jitter delays from destination to source
Positive SD square sum	Square sum of positive jitter delays from source to destination
Positive DS square sum	Square sum of positive jitter delays from destination to source
Min negative SD	Minimum absolute value among negative jitter delays from source to destination
Min negative DS	Minimum absolute value among negative jitter delays from destination to source
Max negative SD	Maximum absolute value among negative jitter delays from source to destination
Max negative DS	Maximum absolute value among negative jitter delays from destination to source
Negative SD number	Number of negative jitter delays from source to destination
Negative DS number	Number of negative jitter delays from destination to source
Negative SD sum	Sum of absolute values of negative jitter delays from source to destination
Negative DS sum	Sum of absolute values of negative jitter delays from destination to source

Field	Description
Negative SD average	Average absolute value of negative jitter delays from source to destination
Negative DS average	Average absolute value of negative jitter delays from destination to source
Negative SD square sum	Square sum of negative jitter delays from source to destination
Negative DS square sum	Square sum of negative jitter delays from destination to source
One way results	Uni-direction delay test result, displayed in a UDP jitter or voice test
Max SD delay	Maximum delay from source to destination
Max DS delay	Maximum delay from destination to source
Min SD delay	Minimum delay from source to destination
Min DS delay	Minimum delay from destination to source
Number of SD delay	Number of delays from source to destination
Number of DS delay	Number of delays from destination to source
Sum of SD delay	Sum of delays from source to destination
Sum of DS delay	Sum of delays from destination to source
Square sum of SD delay	Square sum of delays from source to destination
Square sum of DS delay	Square sum of delays from destination to source
SD lost packet(s)	Number of lost packets from the source to the destination
DS lost packet(s)	Number of lost packets from the destination to the source
Lost packet(s) for unknown reason	Number of lost packets for unknown reasons
Voice scores	Voice parameters, displayed only in a voice test
MOS value	MOS value calculated for a voice test
ICPIF value	ICPIF value calculated for a voice test

display nqa statistics

Syntax

display nqa statistics [*admin-name operation-tag*]

View

Any view

Default Level

2: System level

Parameters

admin-name operation-tag: Displays statistics of the specified test group. If this argument is not specified, statistics of all test groups are displayed. *admin-name* represents the name of the administrator who creates the NQA operation. It is a string of 1 to 32 characters, case-insensitive. *operation-tag* represents the test operation tag. It is a string of 1 to 32 characters, case-insensitive.

Description

Use the **display nqa statistics** command to display statistics of NQA test or tests.

After the test operation begins, if not all the probes in the first test have been finished, statistics cannot be generated. In this case, if you display the statistics using this command, the statistics is displayed as all 0s.

Examples

Display statistics of UDP jitter tests.

```
<Sysname> display nqa statistics admin test
  NQA entry(admin admin, tag test) test statistics:
    NO. : 1
    Destination IP address: 192.168.1.42
      Start time: 2008-05-29 11:33:29.9
      Life time: 8
      Send operation times: 70           Receive response times: 70
      Min/Max/Average round trip time: 1/63/19
      Square-Sum of round trip time: 36330
    Extended results:
      Packet lost in test: 0%
      Failures due to timeout: 0
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    UDP-jitter results:
     RTT number: 70
      Min positive SD: 1                 Min positive DS: 1
      Max positive SD: 24                Max positive DS: 22
      Positive SD number: 34              Positive DS number: 27
      Positive SD sum: 415               Positive DS sum: 362
      Positive SD average: 12             Positive DS average: 13
      Positive SD square sum: 6593         Positive DS square sum: 6450
      Min negative SD: 1                 Min negative DS: 1
      Max negative SD: 40                Max negative DS: 64
      Negative SD number: 28              Negative DS number: 35
      Negative SD sum: 28                Negative DS sum: 35
      Negative SD average: 13             Negative DS average: 12
      Negative SD square sum: 7814         Negative DS square sum: 420
    One way results:
```

```
    Max SD delay: 31                  Max DS delay: 31
    Min SD delay: 7                   Min DS delay: 7
    Number of SD delay: 70            Number of DS delay: 70
    Sum of SD delay: 628              Sum of DS delay: 656
    Square sum of SD delay: 8156      Square sum of DS delay: 8704
    SD lost packet(s): 0              DS lost packet(s): 0
    Lost packet(s) for unknown reason: 0
```

Display statistics of voice tests.

```
<Sysname> display nqa statistics admin test
  NQA entry(admin admin, tag test) test statistics:
    NO. : 1
    Destination IP address: 192.168.1.42
      Start time: 2008-05-29 11:00:03.6
      Life time: 638
      Send operation times: 10000        Receive response times: 0
      Min/Max/Average round trip time: 0/0/0
      Square-Sum of round trip time: 0
    Extended results:
      Packet lost in test: 100%
      Failures due to timeout: 10000
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packet(s) arrived late: 0
    Voice results:
     RTT number: 0
      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 average: 0            Positive DS average: 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 average: 0            Negative DS average: 0
      Negative SD square sum: 0         Negative DS square sum: 0
    One way results:
      Max SD delay: 0                   Max DS delay: 0
      Min SD delay: 0                   Min DS delay: 0
      Number of SD delay: 0             Number of DS delay: 0
      Sum of SD delay: 0                Sum of DS delay: 0
      Square sum of SD delay: 0         Square sum of DS delay: 0
      SD lost packet(s): 0              DS lost packet(s): 0
```

```
  Lost packet(s) for unknown reason: 10000
Voice scores:
  Max MOS value: 0.99                Min MOS value: 0.99
  Max ICPIF value: 87                Min ICPIF value: 87
```

Table 18-4 display nqa statistics command output description

Field	Description
No.	Statistics group number
Destination IP address	IP address of the destination
Start time	Test start time
Life time	Duration of the test, in seconds
Send operation times	Number of probe packets sent
Receive response times	Number of response packets received
Min/Max/Average round trip time	Minimum/maximum/average roundtrip time, in milliseconds
Square-Sum of round trip time	Square sum of roundtrip time
Packet lost in test	Average packet loss ratio
Failures due to timeout	Number of timeout occurrences in a test
Failures due to disconnect	Number of disconnections by the peer
Failures due to no connection	Number of failures to connect with the peer
Failures due to sequence error	Number of failures owing to out-of-sequence packets
Failures due to internal error	Number of failures owing to internal errors
Failures due to other errors	Failures due to other errors
Packet(s) arrived late	Number of response packets received after a probe times out
UDP-jitter results	UDP jitter test results, available only in UDP jitter tests.
Voice results	Voice test results, available only in voice tests.
RTT number	Number of response packets received
Min positive SD	Minimum positive jitter delay from source to destination
Min positive DS	Minimum positive jitter delay from destination to source
Max positive SD	Maximum positive jitter delay from source to destination
Max positive DS	Maximum positive jitter delay from destination to source
Positive SD number	Number of positive jitter delays from source to destination
Positive DS number	Number of positive jitter delays from destination to source
Positive SD sum	Sum of positive jitter delays from source to destination
Positive DS sum	Sum of positive jitter delays from destination to source
Positive SD average	Average of positive jitter delays from source to destination
Positive DS average	Average of positive jitter delays from destination to source
Positive SD square sum	Square sum of positive jitter delays from source to destination

Field	Description
Positive DS square sum	Square sum of positive jitter delays from destination to source
Min negative SD	Minimum absolute value among negative jitter delays from source to destination
Min negative DS	Minimum absolute value among negative jitter delays from destination to source
Max negative SD	Maximum absolute value among negative jitter delays from source to destination
Max negative DS	Maximum absolute value among negative jitter delays from destination to source
Negative SD number	Number of negative jitter delays from source to destination
Negative DS number	Number of negative jitter delays from destination to source
Negative SD sum	Sum of absolute values of negative jitter delays from source to destination
Negative DS sum	Sum of absolute values of negative jitter delays from destination to source
Negative SD average	Average absolute value of negative jitter delays from source to destination
Negative DS average	Average absolute value of negative jitter delays from destination to source
Negative SD square sum	Square sum of negative jitter delays from source to destination
Negative DS square sum	Square sum of negative jitter delays from destination to source
One way results	Uni-direction delay test result, displayed on in a UDP-Jitter or voice test
Max SD delay	Maximum delay from source to destination
Max DS delay	Maximum delay from destination to source
Min SD delay	Minimum delay from source to destination
Min DS delay	Minimum delay from destination to source
Number of SD delay	Number of delays from source to destination
Number of DS delay	Number of delays from destination to source
Sum of SD delay	Sum of delays from source to destination
Sum of DS delay	Sum of delays from destination to source
Square sum of SD delay	Square sum of delays from source to destination
Square sum of DS delay	Square sum of delays from destination to source
SD lost packet(s)	Number of lost packets from the source to the destination
DS lost packet(s)	Number of lost packets from the destination to the source
Lost packet(s) for unknown reason	Number of lost packets for unknown reasons
Voice scores	Voice parameters, displayed only in a voice test

filename

Syntax

filename *filename*

undo filename

View

FTP test type view

Default Level

2: System level

Parameters

filename: Name of the file transferred between the FTP server and the FTP client, a string of 1 to 200 characters. It is case sensitive.

Description

Use the **filename** command to specify a file to be transferred between the FTP server and the FTP client.

Use the **undo filename** command to restore the default.

By default, no file is specified.

Examples

Specify the file to be transferred between the FTP server and the FTP client as config.txt.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] filename config.txt
```

frequency

Syntax

frequency *interval*

undo frequency

View

Any NQA test type view

Default Level

2: System level

Parameters

interval: Interval between two consecutive tests, in milliseconds, in the range 0 to 604800000. If the interval is 0, it indicates that only one test is performed, and no statistics are generated.

Description

Use the **frequency** command to configure the interval between two consecutive tests for a test group.

Use the **undo frequency** command to restore the default.

By default, the interval between two consecutive voice tests is 60000 milliseconds, and the interval between two consecutive tests of other types is 0 milliseconds, that is, only one test is performed.

After you use the **nqa schedule** command to start an NQA test, one test is started at *interval*.

If the last test is not completed when the interval specified by the **frequency** command is reached, a new test is not started.

Examples

Configure the interval between two consecutive tests as 1000 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] frequency 1000
```

history-records

Syntax

history-records *number*

undo history-records

View

Any NQA test type view

Default Level

2: System level

Parameters

number: Maximum number of history records that can be saved in a test group, in the range 0 to 50.

Description

Use the **history-records** command to configure the maximum number of history records that can be saved in a test group.

Use the **undo history-records** command to restore the default.

By default, the maximum number of records that can be saved in a test group is 50.

If the number of history records exceeds the maximum number, the earliest history record for a probe will be discarded.

Examples

Configure the maximum number of history records that can be saved in a test group as 10.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-records 10
```

http-version

Syntax

http-version v1.0

undo http-version

View

HTTP test type view

Default Level

2: System level

Parameters

v1.0: The HTTP version is 1.0 in an HTTP test.

Description

Use the **http-version** command to configure the HTTP version used in an HTTP test.

Use the **undo http-version** command to restore the default.

By default, HTTP 1.0 is used in an HTTP test.

Examples

Configure the HTTP version as 1.0 in an HTTP test.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] http-version v1.0
```

next-hop

Syntax

next-hop *ip-address*

undo next-hop

View

ICMP echo test type view

Default Level

2: System level

Parameters

ip-address: IP address of the next hop.

Description

Use the **next-hop** command to configure the next hop IP address for an IP packet.

Use the **undo next-hop** command to remove the configured next hop IP address.

By default, no next hop IP address is configured.

Examples

Configure the next hop IP address as 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] next-hop 10.1.1.1
```

nqa

Syntax

nqa entry *admin-name operation-tag*

undo nqa { **all** | **entry** *admin-name operation-tag* }

View

System view

Default Level

2: System level

Parameters

admin-name: Specifies the name of the administrator who creates the NQA test operation, a string of 1 to 32 characters, with “-” excluded. It is case-insensitive.

operation-tag: Specifies the tag of a test operation, a string of 1 to 32 characters, with “-” excluded. It is case-insensitive.

all: All NQA test groups.

Description

Use the **nqa** command to create an NQA test group and enter NQA test group view.

Use the **undo nqa** command to remove the test group.

Note that if the test type has been configured for the test group, you will directly enter NQA test type view when you execute the **nqa** command.

Examples

Create an NQA test group whose administrator name is **admin** and whose operation tag is **test** and enter NQA test group view.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test]
```

nqa agent enable

Syntax

nqa agent enable

undo nqa agent enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **nqa agent enable** command to enable the NQA client.

Use the **undo nqa agent enable** command to disable the NQA client and stop all the tests being performed.

By default, the NQA client is enabled.

Related commands: **nqa server enable**.

Examples

Enable the NQA client.

```
<Sysname> system-view
[Sysname] nqa agent enable
```

nqa agent max-concurrent

Syntax

nqa agent max-concurrent *number*

undo nqa agent max-concurrent

View

System view

Default Level

2: System level

Parameters

number: Maximum number of the tests that the NQA client can simultaneously perform, in the range 1 to 5. The default value is 2..

Description

Use the **nqa agent max-concurrent** command to configure the maximum number of tests that the NQA client can simultaneously perform.

Use the **undo nqa agent max-concurrent** command to restore the default.

From the beginning to the end of a test, the NQA test is in the test status; from the end of a test to the beginning of the next test, the NQA test is in the waiting status.

Examples

Configure the maximum number of the tests that the NQA client can simultaneously perform as 3.

```
<Sysname> system-view
[Sysname] nqa agent max-concurrent 3
```

nqa schedule

Syntax

nqa schedule *admin-name operation-tag* **start-time** { *hh*:*mm*:*ss* [*yyyy/mm/dd*] | **now** } **lifetime** { *lifetime* | **forever** }

undo nqa schedule *admin-name operation-tag*

View

System view

Default Level

2: System level

Parameters

admin-name: Specifies the name of the administrator who creates the NQA test operation, a string of 1 to 32 characters. It is case-insensitive.

operation-tag: Specifies the test operation tag, a string of 1 to 32 characters. It is case-insensitive.

start-time: Specifies the start time and date of a test.

hh:*mm*:*ss*: Start time of a test.

yyyy/mm/dd: Start date of a test. The default value is the current system time, and *yyyy* ranges from 2000 to 2035.

now: Starts the tests for a test group immediately.

lifetime: Specifies the duration of the test operation.

lifetime: Duration of the test operation in seconds, in the range 1 to 2147483647.

forever: Specifies that the tests are performed for a test group forever.

Description

Use the **nqa schedule** command to configure the test start time and test duration for a test group.

Use the **undo nqa schedule** command to stop the test for the test group.

Note that:

- It is not allowed to enter test group view or test type view after a test group is scheduled.
- A test group performs a test when the system time is between the start time and the end time (the start time plus test duration). If the system time is behind the start time when you execute the **nqa schedule** command, a test is started when the system time reaches the start time; if the system time is between the start time and the end time, a test is started at once; if the system time is ahead of the end time, no test is started. You can use the **display clock** command to view the current system time.

For the related configurations, refer to the **display clock** command in Basic System Configuration Commands in the System Volume.

Examples

Start the tests for the test group with the administrator name **admin** and operation tag **test**. The start time and duration of the tests are 08:08:08 2008/08/08 and 1000 seconds respectively.

```
<Sysname> system-view
[Sysname] nqa schedule admin test start-time 08:08:08 2008/08/08 lifetime 1000
```

operation (FTP test type view)

Syntax

operation { **get** | **put** }

undo operation

View

FTP test type view

Default Level

2: System level

Parameters

get: Obtains a file from the FTP server.

put: Transfers a file to the FTP server.

Description

Use the **operation** command to configure the FTP operation type.

Use the **undo operation** command to restore the default.

By default, the FTP operation type is **get**.

Examples

Configure the FTP operation type as **put**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] operation put
```

operation (HTTP test type view)

Syntax

operation { **get** | **post** }

undo operation

View

HTTP test type view

Default Level

2: System level

Parameters

get: Obtains data from the HTTP server.

post: Transfers data to the HTTP server.

Description

Use the **operation** command to configure the HTTP operation type.

Use the **undo operation** command to restore the default.

By default, the HTTP operation type is **get**.

Examples

Configure the HTTP operation type as **post**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] operation post
```

operation interface

Syntax

operation interface *interface-type interface-number*

undo operation interface

View

DHCP test type view

Default Level

2: System level

Parameters

interface-type interface-number: Type and number of the interface that is performing a DHCP test.

Description

Use the **operation interface** command to specify the interface to perform a DHCP test.

Use the **undo operation interface** command to restore the default.

By default, no interface is specified to perform a DHCP test.

Note that the specified interface must be up; otherwise, the test will fail.

Examples

Specify the interface to perform a DHCP test as VLAN-interface 2.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dhcp
[Sysname-nqa-admin-test-dhcp] operation interface vlan-interface 2
```

password (FTP test type view)

Syntax

password *password*

undo password

View

FTP test type view

Default Level

2: System level

Parameters

password: Password used to log onto the FTP server, a string of 1 to 32 characters. It is case sensitive.

Description

Use the **password** command to configure a password used to log onto the FTP server.

Use the **undo password** command to remove the configured password.

By default, no password is configured for logging onto the FTP server.

Related commands: **username**, **operation**.

Examples

Configure the password used for logging onto the FTP server as **ftpuser**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] password ftpuser
```

probe count

Syntax

probe count *times*

undo probe count

View

DHCP, DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter test type view

Default Level

2: System level

Parameters

times: Number of probes in an NQA test, in the range 1 to 15.

Description

Use the **probe count** command to configure the number of probes in an NQA test.

Use the **undo probe count** command to restore the default.

By default, one probe is performed in an NQA test.

- For a TCP or DLSw test, one probe means one connection;
- For a UDP jitter test or a voice test, the number of packets sent in one probe depends on the **probe packet-number** command;
- For an FTP, HTTP or DHCP test, one probe means to carry out a corresponding function;
- For an ICMP echo or UDP echo test, one packet is sent in one probe;
- For an SNMP test, three packets are sent in a probe.

If the number of probes in a test is greater than 1, the system performs a second probe after it performs the first probe and receives a response packet. If the system does not receive a response packet, it waits for the test timer to expire before performing a second probe. The process is repeated until the specified probes are completed.

Note that this command is not supported in a voice test. Only one probe can be made in a voice test.

Examples

Configure the number of probes in an ICMP echo test as 10.

```
<Sysname> system-view
[Sysname] nqa entry admin-test
[Sysname-nqa-admin-test] type icmp-echo
[Syaname-nqa-admin-test-icmp-echo] probe count 10
```

probe packet-interval

Syntax

probe packet-interval *packet-interval*

undo probe packet-interval

View

UDP jitter, voice test type view

Default Level

2: System level

Parameters

packet-interval: Interval for packets sent in a probe in a test, in milliseconds, in the range 10 to 60000.

Description

Use the **probe packet-interval** command to configure the interval for sending packets in a probe in a test.

Use the **undo probe-interval** command to restore the default.

By default, the interval is 20 milliseconds.

Examples

Configure the interval for sending packets in a probe in a UDP jitter test as 100 milliseconds.

```
<Sysname> system-view
```

```
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Syaname-nqa-admin-test-udp-jitter] probe packet-interval 100
```

probe packet-number

Syntax

probe packet-number *packet-number*

undo probe packet-number

View

UDP jitter, voice test type view

Default Level

2: System level

Parameters

packet-number: Number of packets sent in a UDP jitter probe or a voice probe. For a UDP jitter test, it is in the range 10 to 1000; for a voice test, it is in the range 10 to 60000.

Description

Use the **probe packet-number** command to configure the number of packets sent in a UDP jitter probe or a voice probe.

Use the **undo probe packet-number** command to restore the default.

By default, the number of packets sent in a probe is 10 in a UDP jitter test and 1000 in a voice test.

Examples

Configure the number of packets sent in a UDP jitter probe as 100.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Syaname-nqa-admin-test-udp-jitter] probe packet-number 100
```

probe packet-timeout

Syntax

probe packet-timeout *packet-timeout*

undo probe packet-timeout

View

UDP jitter, voice test type view

Default Level

2: System level

Parameters

packet-timeout: Timeout time for waiting for responses in a UDP jitter or voice test, in the range 10 to 3600000 milliseconds.

Description

Use the **probe packet-timeout** command to configure the timeout time for waiting for responses in a UDP jitter or voice test.

Use the **undo probe packet-timeout** command to restore the default.

By default, the timeout time in a UDP jitter and a voice test is 3000 and 5000 milliseconds respectively.

Examples

Configure the timeout time for waiting for responses in a UDP jitter test as 100 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Syaname-nqa-admin-test-udp-jitter] probe packet-timeout 100
```

probe timeout

Syntax

probe timeout *timeout*

undo probe timeout

View

DHCP, DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo test type view

Default Level

2: System level

Parameters

timeout: Timeout time in a probe except UDP jitter probe, in milliseconds. For an FTP or HTTP probe, the value range is 10 to 86400000; for a DHCP, DLSw, ICMP echo, SNMP, TCP or UDP echo probe, the value range is 10 to 3600000.

Description

Use the **probe timeout** command to configure the timeout time in a probe.

Use the **undo probe timeout** command to restore the default.

By default, the timeout time is 3000 milliseconds.

After an NQA probe begins, if the NQA probe is not finished within the time specified in the **probe timeout** command, then the probe times out.

Examples

Configure the timeout time in a DHCP probe as 10000 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type dhcp
[Syaname-nqa-admin-test-dhcp] probe timeout 10000
```

reaction

Syntax

reaction *item-num* **checked-element probe-fail threshold-type consecutive** *occurrences* [**action-type** { **none** | **trigger-only** }]

undo reaction *item-num*

View

DHCP, DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo test type view

Default Level

2: System level

Parameters

item-num: Number of the reaction entry, in the range 1 to 10.

checked-element: Type of the monitored element in collaboration. At present, the type of the monitored element can be probe failure only.

probe-fail: The type of the monitored element is probe failure.

threshold-type consecutive: Threshold type is consecutive probe failures.

occurrences: Number of consecutive probe failures, in the range 1 to 16.

action-type: Triggered action type, defaulting to **none**.

none: No actions.

trigger-only: Triggers collaboration between other modules only.

Description

Use the **reaction** command to establish a collaboration entry to monitor the probe results of the current test group. If the number of consecutive probe failures reaches the threshold, collaboration with other modules is triggered.

Use the **undo reaction** command to remove the collaboration entry.

By default, no collaboration entries are configured.

Note that:

- You cannot modify the content of a collaboration object using the **reaction** command after the collaboration object is created.
- The collaboration function is not supported in a UDP jitter or voice test.

Related commands: **track** in the *Track Commands* in the *High Availability Volume*.

Examples

Create collaboration object 1. If the number of consecutive probe failures reaches 3, collaboration with other modules is triggered.

```
<Sysname> system-view
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type tcp
[Sysname-nqa-admin-test-tcp] reaction 1 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only
```

reaction trap

Syntax

reaction trap { **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** *cumulate-probe-failures* }

undo reaction trap { **probe-failure** | **test-complete** | **test-failure** }

View

Any NQA test type view

Default Level

2: System level

Parameters

probe-failure *consecutive-probe-failures*: Specifies to send a trap indicating a probe failure to the network management server after consecutive probe failures in an NQA test. *consecutive-probe-failures* is the number of consecutive probe failures in a test, in the range 1 to 15.

test-complete: Specifies to send a trap to indicate that the test is completed.

test-failure *cumulate-probe-failures*: Specifies to send a trap indicating a probe failure to the network management server if the total number of probe failures in an NQA test is larger than or equal to *cumulate-probe-failures*. For one test, the trap is sent only when the test is completed. *cumulate-probe-failures* is the total number of consecutive probe failures in a test, in the range 1 to 15.

Description

Use the **reaction trap** command to configure to send traps to network management server under specified conditions.

Use the **undo reaction trap** command to restore the default.

By default, no traps are sent to the network management server.

Note that only the **reaction trap test-complete** command is supported in a voice test, namely, in a voice test, traps are sent to the NMS only if the test succeeds.

Examples

Configure to send a trap indicating a probe failure after five consecutive probe failures in an ICMP echo test.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction trap probe-failure 5
```

route-option bypass-route

Syntax

route-option bypass-route

undo route-option bypass-route

View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default Level

2: System level

Parameters

None

Description

Use the **route-option bypass-route** command to enable the routing table bypass function to test the direct connectivity to the direct destination.

Use the **undo route-option bypass-route** command to disable the routing table bypass function.

By default, the routing table bypass function is disabled.

Note that after this function is enabled, the routing table is not searched, and the packet is directly sent to the destination in a directly connected network.

Examples

Enable the routing table bypass function.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] route-option bypass-route
```

source interface

Syntax

source interface *interface-type interface-number*

undo source interface

View

ICMP echo test type view

Default Level

2: System level

Parameters

interface-type interface-number: Interface type and the interface number of the source interface of a probe packet.

Description

Use the **source interface** command to specify the IP address of an interface as the source IP address of ICMP echo probe requests.

Use the **undo source interface** command to remove the IP address of an interface as the source IP address of ICMP echo probe requests.

By default, no interface address is specified as the source IP address of ICMP test request packets.

Note that:

- If you use the **source ip** command to configure the source IP address of ICMP probe requests, the **source interface** command is invalid.
- The interface specified by the **source interface** command must be up; otherwise, the probe fails.

Related commands: **source ip**.

Examples

Specify the IP address of interface VLAN-interface 2 as the source IP address of ICMP echo probe requests.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source interface vlan-interface 2
```

source ip

Syntax

source ip *ip-address*

undo source ip

View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default Level

2: System level

Parameters

ip-address: Source IP address of a test operation.

Description

Use the **source ip** command to configure the source IP address of ICMP probe requests in a test operation.

Use the **undo source ip** command to remove the configured source address. That is, the IP address of the interface sending a probe request serves as the source IP address of the probe request.

By default, no source IP address is specified.

Note that:

- For an ICMP echo test, if no source IP address is specified, but the source interface is specified, the IP address of the source interface is taken as the source IP address of ICMP probe requests.

- The source IP address specified by the **source ip** command must be the IP address of an interface on the device, and the interface must be up; otherwise, the test fails.

Related commands: **source interface**.

Examples

Configure the source IP address of an ICMP echo probe request as 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source ip 10.1.1.1
```

source port

Syntax

source port *port-number*

undo source port

View

SNMP, UDP echo, UDP jitter, voice test type view

Default Level

2: System level

Parameters

port-number: Source port number for a test operation, in the range 1 to 50000.

Description

Use the **source port** command to configure the source port of ICMP probe requests in a test operation.

Use the **undo source port** command to remove the configured port number.

By default, no source port number is specified.

Examples

Configure the source port number of a probe request as 8000.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] source port 8000
```

statistics hold-time

Syntax

statistics hold-time *hold-time*

undo statistics hold-time

View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default Levels

2: System level

Parameters

hold-time: Hold time of a statistics group in minutes, in the range 1 to 1440.

Description

Use the **statistics hold-time** command to configure the hold time of a statistics group.

Use the **undo statistics hold-time** command to restore the default.

By default, the hold time of a statistics group is 120 minutes.

A statistics group has the aging mechanism. A statistics group will be deleted after it is kept for a period of time so that information of a new statistics group will be recorded.

Note that this command is supported on all types of tests except DHCP tests.

Examples

Configure the hold time of a statistics group as 3 minutes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics hold-time 3
```

statistics max-group

Syntax

statistics max-group *number*

undo statistics max-group

View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default Levels

2: System level

Parameters

number: Maximum number of statistics groups that can be kept, in the range 0 to 100.

Description

Use the **statistics max-group** command to configure the maximum number of statistics groups that can be kept.

Use the **undo statistics max-group** command to restore the default.

By default, the maximum number of statistics groups that can be kept is 2.

When the number of statistics groups kept reaches the upper limit, if a new statistics group is generated, the statistics group that is kept the longest is deleted.

Note that:

- This command is supported in all tests except DHCP tests.
- The value of 0 indicates that no statistics are collected.

Examples

Configure the maximum number of statistics groups that can be kept as 5.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics max-group 5
```

statistics interval

Syntax

statistics interval *interval*

undo statistics interval

View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default Levels

2: System level

Parameters

interval: Interval for collecting statistics of the test results in minutes, in the range 1 to 35791394.

Description

Use the **statistics interval** command to configure the interval for collecting statistics of the test results.

Use the **undo statistics interval** command to restore the default.

By default, the interval is 60 minutes.

NQA puts the NQA tests completed in a certain interval into one group, and calculates the statistics of the test results of the group. These statistics form a statistics group. You can use the **display nqa statistics** command to display information of the statistics group.

Note that this command is supported on all types of tests except DHCP tests.

Examples

Configure the interval for collecting statistics of the test results as 2 minutes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] statistics interval 2
```

tos

Syntax

tos *value*

undo tos

View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default Level

2: System level

Parameters

value: Value of the ToS field in the IP header in an NQA probe packet, in the range 0 to 255.

Description

Use the **tos** command to configure the value of the ToS field in the IP header in an NQA probe packet.

Use the **undo tos** command to restore the default.

By default, the ToS field in the IP header of an NQA probe packet is 0.

Examples

Configure the ToS field in a IP packet header in an NQA probe packet as 1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] tos 1
```

ttl

Syntax

ttl *value*

undo ttl

View

DLSw, FTP, HTTP, ICMP echo, SNMP, TCP, UDP echo, UDP jitter, voice test type view

Default Level

2: System level

Parameters

value: Maximum number of hops a probe packet traverses in the network, in the range 1 to 255.

Description

Use the **ttl** command to configure the maximum number of hops a probe packet traverses in the network.

Use the **undo ttl** command to restore the default.

By default, the maximum number of hops that a probe packet can traverse in a network is 20.

Note that after you configure the **route-option bypass-route** command, the maximum number of hops a probe packet traverses in the network is 1, and the **ttl** command does not take effect.

Examples

Configure the maximum number of hops that a probe request can traverse in a network as 16.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] ttl 16
```

type

Syntax

type { **dhcp** | **dlsw** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **voice** }

View

NQA test group view

Default Level

2: System level

Parameters

dhcp: DHCP test.

dlsw: DLSw test.

ftp: FTP test.

http: HTTP test.

icmp-echo: ICMP echo test.

snmp: SNMP test.

tcp: TCP test.

udp-echo: UDP echo test.

udp-jitter: UDP jitter test.

voice: Voice test.

Description

Use the **type** command to configure the test type of the current test group and enter test type view.

By default, no test type is configured.

Examples

Configure the test type of a test group as **FTP** and enter test type view.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp]
```

url

Syntax

url *url*

undo url

View

HTTP test type view

Default Level

2: System level

Parameters

url: Website that an HTTP test visits, a string of 1 to 185 characters. It is case sensitive.

Description

Use the **url** command to configure the website an HTTP test visits.

Use the **undo url** command to remove the configured website an HTTP test visits.

Note that the character string of the configured URL cannot contain spaces.

Examples

Configure the website that an HTTP test visits as /index.htm.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] url /index.htm
```

username (FTP test type view)

Syntax

username *username*

undo username

View

FTP test type view

Default Level

2: System level

Parameters

username: Username used to log onto the FTP server, a string of 1 to 32 characters. It is case sensitive.

Description

Use the **username** command to configure a username used to log onto the FTP server.

Use the **undo username** command to remove the configured username.

By default, no username is configured for logging onto the FTP server.

Related commands: **password**, **operation**.

Examples

Configure the login username as **administrator**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] username administrator
```

vpn-instance (ICMP echo test type view)

Syntax

vpn-instance *instance*

undo vpn-instance

View

ICMP echo test type view

Default Level

2: System level

Parameters

instance: VPN instance name, a string of 1 to 31 characters. It is case sensitive.

Description

Use the **vpn-instance** command to specify a VPN instance.

Use the **undo vpn-instance** command to restore the default.

By default, no VPN instance is specified.

After you specify a VPN instance, NQA will test the connectivity of the specified VPN tunnel.

Examples

Specify the VPN instance **vpn1**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] vpn-instance vpn1
```

NQA Server Configuration Commands

Note

You only need to configure the NQA server for UDP jitter, TCP, UDP echo and voice tests.

---

display nqa server status

Syntax

display nqa server status

View

Any view

Default Level

2: System level

Parameters

None

Description

Use the **display nqa server status** command to display NQA server status.

Examples

Display NQA server status.

```
<Sysname> display nqa server status
nqa server is: enabled
tcp-connect:
    IP Address     Port          Status
    2.2.2.2        2000          active
udp-echo:
    IP Address     Port          Status
    3.3.3.3        3000          inactive
```

Table 18-5 display nqa server status command output description

Field	Description
tcp-connect	NQA server status in the NQA TCP test
udp-echo	NQA server status in the NQA UDP test
IP Address	IP address specified for the TCP/UDP listening service on the NQA server
Port	Port number of the TCP/UDP listening service on the NQA server
Status	Listening service status: **active**: Listening service is ready; **inactive**: Listening service is not ready.

nqa server enable

Syntax

nqa server enable

undo nqa server enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **nqa server enable** command to enable the NQA server.

Use the **undo nqa server enable** command to disable the NQA server.

By default, the NQA server is disabled.

Related commands: **nqa server tcp-connect**, **nqa server udp-echo** and **display nqa server status**.

Examples

Enable the NQA server.

```
<Sysname> system-view
[Sysname] nqa server enable
```

nqa server tcp-connect

Syntax

nqa server tcp-connect *ip-address port-number*

undo nqa server tcp-connect *ip-address port-number*

View

System view

Default Level

2: System level

Parameters

ip-address: IP address specified for the TCP listening service on the NQA server.

port-number: Port number specified for the TCP listening service on the NQA server, in the range 1 to 50000.-

Description

Use the **nqa-server tcp-connect** command to create a TCP listening service on the NQA server.

Use the **undo nqa-server tcp-connect** command to remove the TCP listening service created.

Note that:

- You need to configure the command on the NQA server for TCP tests only.

- The IP address and port number must be consistent with those on the NQA client and must be different from those for an existing listening service.
- The IP address must be that of an interface on the NQA server. Otherwise, the configuration will be invalid.

Related commands: **nqa server enable** and **display nqa server status**.

Examples

Create a TCP listening service by using the IP address 169.254.10.2 and port 9000.

```
<Sysname> system-view
[Sysname] nqa server tcp-connect 169.254.10.2 9000
```

nqa server udp-echo

Syntax

nqa server udp-echo *ip-address port-number*

undo nqa server udp-echo *ip-address port-number*

View

System view

Default Level

2: System level

Parameters

ip-address: IP address specified for the UDP listening service on the NQA server.

port-number: Port number specified for the UDP listening service on the NQA server, in the range 1 to 50000.

Description

Use the **nqa-server udp-echo** command to create a UDP listening service on the NQA server.

Use the **undo nqa-server udp-echo** command to remove the UDP listening service created.

Note that:

- You need to configure the command on the NQA server for UDP jitter, UDP echo and voice tests only.
- The IP address and port number must be consistent with those configured on the NQA client and must be different from those of an existing listening service.
- The IP address must be that of an interface on the NQA server. Otherwise, the configuration will be invalid.

Related commands: **nqa server enable** and **display nqa server status**.

Examples

Create a UDP listening service by using the IP address 169.254.10.2 and port 9000.

```
<Sysname> system-view
[Sysname] nqa server udp-echo 169.254.10.2 9000
```

19 NTP Configuration Commands

NTP Configuration Commands

display ntp-service sessions

Syntax

display ntp-service sessions [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

verbose: Displays the detailed information of all NTP sessions. If you do not specify this keyword, only the brief information of the NTP sessions will be displayed.

Description

Use the **display ntp-service sessions** command to view the information of all NTP sessions.

Examples

View the brief information of NTP sessions.

```
<Sysname> display ntp-service sessions
    source      reference   stra reach   poll now  offset  delay disper
**************************************************************************
[12345]1.1.1.1    127.127.1.0  3    377    64  178   0.0    40.1   22.8
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

Table 19-1 display ntp-service sessions command output description

Field	Description
source	IP address of the clock source
reference	Reference clock ID of the clock source 1) If the reference clock is the local clock, the value of this field is related to the value of the **stra** field: • When the value of the **stra** field is 0 or 1, this field will be “LOCL”; • When the **stra** field has another value, this filed will be the IP address of the local clock. 2) If the reference clock is the clock of another device on the network, the value of this field will be the IP address of that device.
stra	Stratum level of the clock source, which determines the clock precision. The value range is 1 to 16. The clock precision decreases from stratum 1 to stratum 16. A stratum 1 clock has the highest precision, and a stratum 16 clock is not synchronized and cannot be used as a reference clock.
reach	Reachability count of the clock source. 0 indicates that the clock source in unreachable.
poll	Poll interval in seconds, namely, the maximum interval between successive NTP messages.
now	The length of time from when the last NTP message was received or when the local clock was last updated to the current time The time is in second by default. If the time length is greater than 2048 seconds, it is displayed in minute; if greater than 300 minutes, in hour; if greater than 96 hours, in day.
offset	The offset of the system clock relative to the reference clock, in milliseconds
delay	the roundtrip delay from the local device to the clock source, in milliseconds
disper	The maximum error of the system clock relative to the reference source.
[12345]	1: Clock source selected by the system, namely, the current reference source, with a system clock stratum level less than or equal to 15 2: Stratum level of the clock source is less than or equal to 15. 3: This clock source has passed the clock selection process. 4: This clock source is a candidate clock source. 5: This clock source was created by a configuration command.
Total associations	Total number of associations

Note

When a device is working in the NTP broadcast/multicast server mode, the **display ntp-service sessions** command executed on the device will not display the NTP session information corresponding to the broadcast/multicast server, but the sessions will be counted in the total number of associations.

display ntp-service status

Syntax

display ntp-service status

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ntp-service status** command to view the NTP service status information.

Examples

View the NTP service status information.

```
<Sysname> display ntp-service status
Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 0.00 ms
 Reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

Table 19-2 display ntp-service status command output description

Field	Description
Clock status	Status of the system clock, including • Synchronized: The system clock has been synchronized. • Unsynchronized: The system clock has not been synchronized.
Clock stratum	Stratum level of the system clock
Reference clock ID	After the system clock is synchronized to a remote time server, this field indicates the address of the remote time server; after the system clock is synchronized to a local reference source, this field indicates the address of the local clock source: • When the local clock has a stratum level of 1, the value of this field is “LOCL”; • When the stratum of the local clock has another value, the value of this filed is the IP address of the local clock.
Nominal frequency	The nominal frequency of the local system hardware clock, in Hz

Field	Description
Actual frequency	The actual frequency of the local system hardware clock, in Hz
Clock precision	The precision of the system clock
Clock offset	The offset of the system clock relative to the reference source, in milliseconds
Root delay	The roundtrip delay from the local device to the primary reference source, in milliseconds
Root dispersion	The maximum error of the system clock relative to the primary reference source, in milliseconds
Peer dispersion	The maximum error of the system clock relative to the reference source, in milliseconds
Reference time	Reference timestamp

display ntp-service trace

Syntax

display ntp-service trace

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ntp-service trace** command view the brief information of each NTP server along the NTP server chain from the local device back to the primary reference source.

The **display ntp-service trace** command takes effect only if routes are available between the local device and all the devices on the NTP server chain; otherwise, this command will fail to display all the NTP servers on the NTP chain due to timeout.

Examples

View the brief information of each NTP server from the local device back to the primary reference source.

```
<Sysname> display ntp-service trace
 server 127.0.0.1,stratum 2, offset -0.013500, synch distance 0.03154
 server 133.1.1.1,stratum 1, offset -0.506500, synch distance 0.03429
 refid LOCL
```

The information above shows an NTP server chain for the server 127.0.0.1: The server 127.0.0.1 is synchronized to the server 133.1.1.1, and the server 133.1.1.1 is synchronized to the local clock source.

Table 19-3 display ntp-service trace command output description

Field	Description
server	IP address of the NTP server
stratum	The stratum level of the corresponding system clock
offset	The clock offset relative to the upper-level clock, in seconds
synch distance	The synchronization distance relative to the upper-level clock, in seconds, and calculated from dispersion and roundtrip delay values.
refid	Identifier of the primary reference source. When the stratum level of the primary reference clock is 0, it is displayed as LOCL; otherwise, it is displayed as the IP address of the primary reference clock.

ntp-service access

Syntax

ntp-service access { **peer** | **query** | **server** | **synchronization** } *acl-number*

undo ntp-service access { **peer** | **query** | **server** | **synchronization** }

View

System view

Default Level

2: System level

Parameters

peer: Specifies to permit full access. This level of right permits the peer devices to perform synchronization and control query to the local device and also permits the local device to synchronize its clock to that of a peer device. Control query refers to query of NTP status information, such as alarm information, authentication status, and clock source information.

query: Specifies to permit control query. This level of right permits the peer devices to perform control query to the NTP service on the local device but does not permit a peer device to synchronize its clock to that of the local device.

server: Specifies to permit server access and query. This level of right permits the peer devices to perform synchronization and control query to the local device but does not permit the local device to synchronize its clock to that of a peer device.

synchronization: Specifies to permit server access only. This level of right permits a peer device to synchronize its clock to that of the local device but does not permit the peer devices to perform control query.

acl-number: Basic ACL number, in the range of 2000 to 2999

Description

Use the **ntp-service access** command to configure the access-control right for the peer devices to access the NTP services of the local device.

Use the **undo ntp-service access** command to remove the configured NTP service access-control right to the local device.

By default, the access-control right for the peer devices to access the NTP services of the local device is set to **peer**.

From the highest NTP service access-control right to the lowest one are **peer**, **server**, **synchronization**, and **query**. When a device receives an NTP request, it will match against the access-control right in this order and will use the first matched right.

Note that:

- The **ntp-service access** command provides only a minimum degree of security protection. A more secure method is identity authentication. The related command is **ntp-service authentication enable**.
- Before specifying an ACL number in the **ntp-service access** command, make sure you have already created and configured this ACL.

Examples

Configure the peer devices on subnet 10.10.0.0/16 to have the full access right to the local device.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-basic-2001] quit
[Sysname] ntp-service access peer 2001
```

ntp-service authentication enable

Syntax

ntp-service authentication enable

undo ntp-service authentication enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **ntp-service authentication enable** command to enable NTP authentication.

Use the **undo ntp-service authentication enable** command to disable NTP authentication.

By default, NTP authentication is disabled.

Related commands: **ntp-service authentication-keyid**, **ntp-service reliable authentication-keyid**.

Examples

Enable NTP authentication.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
```

ntp-service authentication-keyid

Syntax

ntp-service authentication-keyid *keyid* **authentication-mode md5** *value*

undo ntp-service authentication-keyid *keyid*

View

System view

Default Level

2: System level

Parameters

keyid: Authentication key ID, in the range of 1 to 4294967295.

authentication-mode md5 *value*: Specifies to use the MD5 algorithm for key authentication, where *value* represents authentication key and is a string of 1 to 32 characters.

Description

Use the **ntp-service authentication-keyid** command to set the NTP authentication key.

Use the **undo ntp-service authentication-keyid** command to remove the set NTP authentication key.

By default, no NTP authentication key is set.

In a network where there is a high security demand, the NTP authentication feature should be enabled for a system running NTP. This feature enhances the network security by means of the client-server key authentication, which prohibits a client from synchronizing with a device that has failed authentication.

After the NTP authentication key is configured, you need to configure the key as a trusted key by using the **ntp-service reliable authentication-keyid** command.

 **Caution**

- Presently the system supports only the MD5 algorithm for key authentication.
- You can set a maximum of 1,024 keys for each device.
- If an NTP authentication key is specified as a trusted key, the key automatically changes to untrusted after you delete the key. In this case, you do not need to execute the **undo ntp-service reliable authentication-keyid** command.

Related commands: **ntp-service reliable authentication-keyid**.

Examples

Set an MD5 authentication key, with the key ID of 10 and key value of **BetterKey**.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 10 authentication-mode md5 BetterKey
```

ntp-service broadcast-client

Syntax

ntp-service broadcast-client

undo ntp-service broadcast-client

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **ntp-service broadcast-client** command to configure the device to work in the NTP broadcast client mode and use the current interface to receive NTP broadcast packets.

Use the **undo ntp-service broadcast-client** command to remove the configuration.

By default, the device does not work in the NTP broadcast client mode.

Examples

Configure the device to work in the broadcast client mode and receive NTP broadcast messages on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-client
```

ntp-service broadcast-server

Syntax

ntp-service broadcast-server [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

View

Interface view

Default Level

2: System level

Parameters

authentication-keyid *keyid*: Specifies the key ID to be used for sending broadcast messages to broadcast clients, where *keyid* is in the range of 1 to 4294967295. This parameter is not meaningful if authentication is not required.

version *number*: Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

Description

Use the **ntp-service broadcast-server** command to configure the device to work in the NTP broadcast server mode and use the current interface to send NTP broadcast packets.

Use the **undo ntp-service broadcast-server** command to remove the configuration.

By default, the device does not work in the NTP broadcast server mode.

Examples

Configure the device to work in the broadcast server mode and send NTP broadcast messages on VLAN-interface 1, using key 4 for encryption, and set the NTP version to 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-server authentication-keyid 4 version 3
```

ntp-service in-interface disable

Syntax

ntp-service in-interface disable

undo ntp-service in-interface disable

View

Interface view

Default Level

2: System level

Parameters

None

Description

Use the **ntp-service in-interface disable** command to disable an interface from receiving NTP messages.

Use the **undo ntp-service in-interface disable** command to restore the default.

By default, all interfaces are enabled to receive NTP messages.

Examples

Disable VLAN-interface 1 from receiving NTP messages.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service in-interface disable
```

ntp-service max-dynamic-sessions

Syntax

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

View

System view

Default Level

2: System level

Parameters

number: Maximum number of dynamic NTP sessions that are allowed to be established, in the range of 0 to 100.

Description

Use the **ntp-service max-dynamic-sessions** command to set the maximum number of dynamic NTP sessions that are allowed to be established locally.

Use the **undo ntp-service max-dynamic-sessions** command to restore the maximum number of dynamic NTP sessions to the system default.

By default, the number is 100.

A single device can have a maximum of 128 associations at the same time, including static associations and dynamic associations. A static association refers to an association that a user has manually created by using an NTP command, while a dynamic association is a temporary association created by the system during operation. A dynamic association will be removed if the system fails to receive messages from it over a specific long time. In the client/server mode, for example, when you carry out a command to synchronize the time to a server, the system will create a static association, and the server will just respond passively upon the receipt of a message, rather than creating an association (static or dynamic). In the symmetric mode, static associations will be created at the symmetric-active peer side, and dynamic associations will be created at the symmetric-passive peer side; in the broadcast or multicast mode, static associations will be created at the server side, and dynamic associations will be created at the client side.

Examples

Set the maximum number of dynamic NTP sessions allowed to be established to 50.

```
<Sysname> system-view
[Sysname] ntp-service max-dynamic-sessions 50
```

ntp-service multicast-client

Syntax

ntp-service multicast-client [*ip-address*]

undo ntp-service multicast-client [*ip-address*]

View

Interface view

Default Level

2: System level

Parameters

ip-address: Multicast IP address, defaulting to 224.0.1.1.

Description

Use the **ntp-service multicast-client** command to configure the device to work in the NTP multicast client mode and use the current interface to receive NTP multicast packets.

Use the **undo ntp-service multicast-client** command to remove the configuration.

By default, the device does not work in the NTP multicast client mode.

Examples

Configure the device to work in the multicast client mode and receive NTP multicast messages on VLAN-interface 1, and set the multicast address to 224.0.1.1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-client 224.0.1.1
```

ntp-service multicast-server

Syntax

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

undo ntp-service multicast-server [*ip-address*]

View

Interface view

Default Level

2: System level

Parameters

ip-address: Multicast IP address, defaulting to 224.0.1.1.

authentication-keyid *keyid*: Specifies the key ID to be used for sending multicast messages to multicast clients, where *keyid* is in the range of 1 to 4294967295. This parameter is not meaningful if authentication is not required.

ttl *ttl-number*: Specifies the TTL of NTP multicast messages, where *ttl-number* is in the range of 1 to 255 and defaults to 16.

version *number*: Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

Description

Use the **ntp-service multicast-server** command to configure the device to work in the NTP multicast server mode and use the current interface to send NTP multicast packets.

Use the **undo ntp-service multicast-server** command to remove the configuration.

By default, the device does not work in the NTP multicast server mode.

Examples

Configure the device to work in the multicast server mode and send NTP multicast messages on VLAN-interface 1 to the multicast address 224.0.1.1, using key 4 for encryption, and set the NTP version to 3.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-server 224.0.1.1 version 3
authentication-keyid 4
```

ntp-service reliable authentication-keyid

Syntax

ntp-service reliable authentication-keyid *keyid*

undo ntp-service reliable authentication-keyid *keyid*

View

System view

Default Level

2: System level

Parameters

keyid: Authentication key number, in the range of 1 to 4294967295.

Description

Use the **ntp-service reliable authentication-keyid** command to specify that the created authentication key is a trusted key. When NTP authentication is enabled, a client can be synchronized only to a server that can provide a trusted authentication key.

Use the **undo ntp-service reliable authentication-keyid** command to remove the configuration.

No authentication key is configured to be trusted by default.

Examples

Enable NTP authentication, specify to use MD5 encryption algorithm, with the key ID of 37 and key value of **BetterKey**.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 37 authentication-mode md5 BetterKey
```

Specify this key as a trusted key.

```
[Sysname] ntp-service reliable authentication-keyid 37
```

ntp-service source-interface

Syntax

ntp-service source-interface *interface-type interface-number*

undo ntp-service source-interface

View

System view

Default Level

2: System level

Parameters

interface-type interface-number: Specifies an interface by its interface type and interface number.

Description

Use the **ntp-service source-interface** command to specify the source interface for NTP messages.

Use the **undo ntp-service source-interface** command to restore the default.

By default, no source interface is specified for NTP messages, and the system uses the IP address of the interface determined by the matched route as the source IP address of NTP messages.

If you do not wish the IP address of a certain interface on the local device to become the destination address of response messages, you can use this command to specify the source interface for NTP messages, so that the source IP address in NTP messages is the primary IP address of this interface.

Examples

Specify the source interface of NTP messages as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ntp-service source-interface vlan-interface 1
```

ntp-service unicast-peer

Syntax

ntp-service unicast-peer [**vpn-instance** *vpn-instance-name*] { *ip-address* | *peer-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-peer [**vpn-instance** *vpn-instance-name*] { *ip-address* | *peer-name* }

View

System view

Default Level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, where *vpn-instance-name* is a string of 1 to 31 characters.

ip-address: IP address of the symmetric-passive peer. It must be a unicast address, rather than a broadcast address, a multicast address or the IP address of the local clock.

peer-name: Host name of the symmetric-passive peer, a string of 1 to 20 characters.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the peer, where *keyid* is in the range of 1 to 4294967295.

priority: Specifies the peer designated by *ip-address* or *peer-name* as the first choice under the same condition.

source-interface *interface-type interface-number*: Specifies the source interface for NTP messages. In an NTP message the local device sends to its peer, the source IP address is the primary IP address of this interface. *interface-type interface-number* represents the interface type and number.

version *number*: Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

Description

Use the **ntp-service unicast-peer** command to designate a symmetric-passive peer for the device.

Use the **undo ntp-service unicast-peer** command to remove the symmetric-passive peer designated for the device.

No symmetric-passive peer is designated for the device by default.

Note

- To synchronize the switch to another device in a VPN, you need to provide **vpn-instance** *vpn-instance-name* in your command.
- If you include **vpn-instance** *vpn-instance-name* in the **undo ntp-service unicast-peer** command, the command will remove the symmetric-passive peer with the IP address of *ip-address* in the specified VPN; if you do not include **vpn-instance** *vpn-instance-name* in this command, the command will remove the symmetric-passive peer with the IP address of *ip-address* in the public network.

Examples

Designate the device with the IP address of 10.1.1.1 as the symmetric-passive peer of the device, configure the device to run NTP version 3, and specify the source interface of NTP messages as VLAN-interface 1.

```
<Sysname> system-view
[Sysname] ntp-service unicast-peer 10.1.1.1 version 3 source-interface vlan-interface 1
```

ntp-service unicast-server

Syntax

ntp-service unicast-server [**vpn-instance** *vpn-instance-name*] { *ip-address* | *server-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-server [**vpn-instance** *vpn-instance-name*] { *ip-address* | *server-name* }

View

System view

Default Level

2: System level

Parameters

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, where *vpn-instance-name* is a string of 1 to 31 characters.

ip-address: IP address of the NTP server. It must be a unicast address, rather than a broadcast address, a multicast address or the IP address of the local clock.

server-name: Host name of the NTP server, a string of 1 to 20 characters.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server, where *keyid* is in the range of 1 to 4294967295.

priority: Specifies this NTP server as the first choice under the same condition.

source-interface *interface-type interface-number*: Specifies the source interface for NTP messages. In an NTP message the local device sends to the NTP server, the source IP address is the primary IP address of this interface. *interface-type interface-number* represents the interface type and number.

version *number*: Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

Description

Use the **ntp-service unicast-server** command to designate an NTP server for the device.

Use the **undo ntp-service unicast-server** command to remove an NTP server designated for the device.

No NTP server is designated for the device by default.

Note

- To synchronize the switch to another device in a VPN, you need to provide **vpn-instance** *vpn-instance-name* in your command.
- If you include **vpn-instance** *vpn-instance-name* in the **undo ntp-service unicast-server** command, the command will remove the NTP server with the IP address of *ip-address* in the specified VPN; if you do not include **vpn-instance** *vpn-instance-name* in this command, the command will remove the NTP server with the IP address of *ip-address* in the public network.

Examples

Designate NTP server 10.1.1.1 for the device, and configure the device to run NTP version 3.

```
<Sysname> system-view
[Sysname] ntp-service unicast-server 10.1.1.1 version 3
```

20 Cluster Management Configuration Commands

NDP Configuration Commands

display ndp

Syntax

display ndp [**interface** *interface-list*]

View

Any view

Default Level

1: Monitor level

Parameters

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>,where, *interface-type* is port type and *interface-number* is port number, and &<1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

Description

Use the **display ndp** command to display NDP configuration information, which includes the interval to send NDP packets, the time for the receiving device to hold NDP information and the information about the neighbors of all ports.

Examples

Display NDP configuration information.

```
<Sysname> display ndp
Neighbor Discovery Protocol is enabled.
 Neighbor Discovery Protocol Ver: 1, Hello Timer: 60(s), Aging Timer: 180(s)
 Interface: GigabitEthernet1/0/1
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/2
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/3
    Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/4
    Status: Enabled, Pkts Snd: 28440, Pkts Rvd: 27347, Pkts Err: 0
```

```
   Neighbor 1:  Aging Time: 122(s)
      MAC Address : 000f-e200-2579
      Host Name   : Sysname
      Port Name   : GigabitEthernet1/0/4
      Software Ver: ESS 2200
      Device Name : Switch 4210G PWR 48-Port
      Port Duplex : AUTO
      Product Ver : Switch 4210G PWR 48-Port-Release2202
      BootROM Ver : 505


 Interface: GigabitEthernet1/0/5
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/6
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/7
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/8
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/9
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

Interface: GigabitEthernet1/0/10
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/11
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/12
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/13
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/14
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/15
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/16
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/17
```

```
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/18
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/19
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/20
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/21
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/22
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/23
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitEthernet1/0/24
   Status: Enabled, Pkts Snd: 0, Pkts Rvd: 0, Pkts Err: 0

 Interface: GigabitGigabitEthernet1/0/1
   Status: Enabled, Pkts Snd: 28438, Pkts Rvd: 54160, Pkts Err: 0
   Neighbor 1:  Aging Time: 176(s)
      MAC Address : 000f-cbb8-9528
      Host Name   : Sysname
      Port Name   : GigabitGigabitEthernet1/0/2
      Software Ver: V600R006B02D076SP03
      Device Name : 3Com S7902E
      Port Duplex : AUTO
      Product Ver : 005


 Interface: GigabitGigabitEthernet1/0/2
Status: Enabled, Pkts Snd: 1, Pkts Rvd: 1, Pkts Err: 0
```

Table 20-1 display ndp command output description

Field	Description
Neighbor Discovery Protocol is enabled	NDP is enabled globally on the current device.
Neighbor Discovery Protocol Ver	Version of NDP
Hello Timer	Interval to send NDP packets
Aging Timer	The time for the receiving device to hold NDP information
Interface	A specified port

Field	Description
Status	NDP state of a port
Pkts Snd	Number of the NDP packets sent through the port
Pkts Rvd	Number of the NDP packets received on the port
Pkts Err	Number of the error NDP packets received
Neighbor 1: Aging Time	Aging time of the NDP information of a neighbor device
MAC Address	MAC address of a neighbor device
Host Name	Host name of a neighbor device
Port Name	Port name of a neighbor device
Software Ver	Software version of the neighbor device
Device Name	Device name of a neighbor device
Port Duplex	Port duplex mode of a neighbor device
Product Ver	Product version of a neighbor device
BootROM Ver	Boot ROM version of a neighbor device

ndp enable

Syntax

In Ethernet interface view or Layer 2 aggregate interface view:

ndp enable

undo ndp enable

In system view:

ndp enable [**interface** *interface-list*]

undo ndp enable [**interface** *interface-list*]

View

System view, Ethernet interface view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

Description

Use the **ndp enable** command to enable NDP.

Use the **undo ndp enable** command to disable this feature.

By default, NDP is enabled globally and also on all ports.

Note that:

- When being executed in system view, the **ndp enable** command enables NDP globally if you do not specify the **interface** keyword; if you specify the **interface** keyword, the command enables NDP for the specified Ethernet port(s).
- When being executed in interface view, this command enables NDP for the current port only.
- Configured in Layer 2 aggregate interface view, the configuration will not take effect on the member ports of the aggregation group that corresponds to the aggregate interface; configured on a member port of an aggregation group, the configuration will take effect only after the member port quit the aggregation group. For description of aggregation configurations, refer to *Link Aggregation Configuration* in the *Access Volume*.

Examples

Enable NDP globally.

```
<Sysname> system-view
[Sysname] ndp enable
```

Enable NDP for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ndp enable
```

ndp timer aging

Syntax

ndp timer aging *aging-time*

undo ndp timer aging

View

System view

Default Level

2: System level

Parameters

aging-time: Time for a device to keep the NDP packets it receives, in the range 5 to 255 seconds.

Description

Use the **ndp timer aging** command to specify the time that a device should keep the NDP packets it received from the adjacent device.

Use the **undo timer aging** command to restore the default.

By default, the time that a receiving device should keep the NDP packets is 180 seconds.

Note that the time for the receiving device to hold NDP packets cannot be shorter than the interval to send NDP packets; otherwise, the NDP table may become instable.

Related commands: **ndp timer hello**.

Examples

Configure the time that a receiving device should keep the NDP packets as 60 seconds.

```
<Sysname> system-view
[Sysname] ndp timer aging 60
```

ndp timer hello

Syntax

ndp timer hello *hello-time*

undo ndp timer hello

View

System view

Default Level

2: System level

Parameters

hello-time: Interval to send NDP packets, in the range 5 to 254 seconds.

Description

Use the **ndp timer hello** command to set the interval to send NDP packets.

Use the **undo ndp timer hello** command to restore the default.

By default, the interval to send NDP packets is 60 seconds.

Note that the interval for sending NDP packets cannot be longer than the time for the receiving device to hold NDP packets; otherwise, the NDP table may become instable.

Related commands: **ndp timer aging**.

Examples

Set the interval to send NDP packets to 80 seconds.

```
<Sysname> system-view
[Sysname] ndp timer hello 80
```

reset ndp statistics

Syntax

reset ndp statistics [**interface** *interface-list*]

View

User view

Default Level

2: System level

Parameters

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument.

Description

Use the **reset ndp statistics** command to clear NDP statistics.

If no **interface** *interface-list* is specified, NDP statistics of all ports are cleared; otherwise, NDP statistics of a specified port are cleared.

Examples

Clear NDP statistics of all ports.

```
<Sysname> reset ndp statistics
```

NTDP Configuration Commands

display ntdp

Syntax

display ntdp

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ntdp** command to display NTDP configuration information.

Examples

Display the global NTDP information.

```
<Sysname> display ntdp
 NTDP is running.
 Hops     : 4
 Timer    : 1 min(disable)
 Hop Delay : 100 ms
 Port Delay: 10 ms
 Last collection total time: 92ms
```

Table 20-2 display ntdp command output description

Field	Description
NTDP is running	NTDP is enabled globally on the local device.
Hops	Hop count for topology collection
Timer	Interval to collect topology information (after the cluster is created)
disable	Indicates the device is not a management device and unable to perform periodical topology collection
Hop Delay	Delay time for the device to forward topology collection requests
Port Delay	Delay time for a topology-collection request to be forwarded through a port
Last collection total time	Time cost during the last collection

display ntdp device-list

Syntax

display ntdp device-list [**verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

verbose: Displays the detailed device information.

Description

Use the **display ntdp device-list** command to display the device information collected through NTDP.

Note that the information displayed may not be that of the latest device if you do not execute the **ntdp explore** command before using this command.

Examples

Display the device list collected through NTDP.

```
<Sysname> display ntdp device-list
MAC           HOP  IP               Device
 000f-e200-3133  2                   Switch 4200G
 000f-e20f-c415  2   31.31.31.5/24     Switch 4200G
 000f-e200-2579  1                   Switch 4200G
 000f-e200-1751  0   31.31.31.1/24     Switch 4200G
 00e0-fd00-0043  2                   Sysname S3528P
 000f-e200-3199  3                   Switch 4200G
```

Table 20-3 display ntdp device-list command output description

Field	Description
MAC	MAC address of a device
HOP	Hops to the collecting device
IP	IP address and mask length of the management VLAN interface on the device
Device	Device name

Display the detailed device information collected through NTDP.

```
<aabbcc_0.3Com> display ntdp device-list verbose
 Hostname  : 4210G
 MAC       : 000f-e268-8322
 Device    : Switch 4210G 24-Port
 IP        : 192.168.0.1/16
 Version   :
  3Com Corporation
  3Com OS Software Version 5.20 Release 2202P17 Release 2202P17
  Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved.
  Switch 4210G 24-Port V300R001B01D021

--------------------------------------------------------------------------
 Hop       : 2
 Cluster   :  Independent device

 Peer MAC      Peer Port ID            Native Port ID          Speed Duplex
 00e0-fc00-5111 GigabitEthernet1/0/12    GigabitEthernet1/0/22    1000  FULL
------------------------------------------------------------------------------
```

Table 20-4 display ntdp device-list verbose command output description

Field	Description
Hostname	System name of the device
MAC	MAC address of the device
Hop	Hops from the current device to the device that collect topology information
Device	Device name
IP	IP address and subnet mask length of the management VLAN interface on the device
Version	Version information
Cluster	Role of the device in the cluster
Cluster : Member switch of cluster aabbcc	The device is a member device of the cluster **aabbcc**.
Administrator MAC	MAC address of the management device
Administrator switch of cluster aabbcc	The device is the management device of the cluster **aabbcc**.

Field	Description
Peer MAC	MAC address of a neighbor device
Peer Port ID	Name of the peer port connected to the local port
Native Port ID	Name of the local port to which a neighbor device is connected
Speed	Speed of the local port to which a neighbor device is connected
Duplex	Duplex mode of the local port to which a neighbor device is connected

display ntdp single-device mac-address

Syntax

display ntdp single-device mac-address *mac-address*

View

Any view

Default Level

1: Monitor level

Parameters

mac-address: MAC address of the device, in the format of H-H-H.

Description

Use the **display ntdp single-device mac-address** command to view the detailed NTDP information of a specified device.

Examples

Display the detailed NTDP information of the device with a MAC address of 000f-e200-5111.

```
<Sysname> display ntdp single-device mac-address 000f-e200-5111

 Hostname  : test_2.Sysname
 MAC       : 000f-e234-5678
 Device    : 3Com S7902E
 IP        : 192.168.0.71/24
 Version   :
  3Com Corporation
  3Com OS Software Version 3ComComware Release 520 Test 6610
  Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved.
  3Com S7902E V600R006B02D076SP03, Test 6610

------------------------------------------------------------------
 Hop       : 2
 Cluster   :  Member device of cluster test , Administrator MAC: 000f-e2d2-58fb

 Peer MAC      Peer Port ID           Native Port ID          Speed Duplex
```

```
00e0-fc00-5111 GigabitEthernet1/0/1     GigabitEthernet2/0/45     1000  FULL
```

Refer to Table 20-4 for the description of the above prompt information.

ntdp enable

Syntax

ntdp enable

undo ntdp enable

View

System view, Ethernet interface view, Layer 2 aggregate interface view

Default Level

2: System level

Parameters

None

Description

Use the **ntdp enable** command to enable NTDP.

Use the **undo ntdp enable** command to disable NTDP.

By default, NTDP is enabled globally and on all ports.

Note that:

- Execution of the command in system view enables the global NTDP; execution of the command in interface view enables NTDP of the current port.
- Configured in Layer 2 aggregate interface view, the configuration will not take effect on the member ports of the aggregation group that corresponds to the aggregate interface; configured on a member port of an aggregation group, the configuration will take effect only after the member port quit the aggregation group. For description of aggregation configurations, refer to *Link Aggregation Configuration* in the *Access Volume*.

Examples

Enable NTDP globally.

```
<Sysname> system-view
[Sysname] ntdp enable
```

Enable NTDP for port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ntdp enable
```

ntdp explore

Syntax

ntdp explore

View

User view

Default Level

2: System level

Parameters

None

Description

Use the **ntdp explore** command to start topology information collection manually.

Examples

Start the topology information collection.

```
<Sysname> ntdp explore
```

ntdp hop

Syntax

ntdp hop *hop-value*

undo ntdp hop

View

System view

Default Level

2: System level

Parameters

hop-value: Maximum hop for collecting topology information, in the range 1 to 16.

Description

Use the **ntdp hop** command to set maximum hop for collecting topology information.

Use the **undo ntdp hop** command to restore the default.

By default, the value is 3.

Note that this command is only applicable to the topology-collecting device. A bigger number of hops requires more memory of the topology-collecting device.

Examples

Set the hop count for topology information collection to 5.

```
<Sysname> system-view
[Sysname] ntdp hop 5
```

ntdp timer

Syntax

ntdp timer *interval-time*

undo ntdp timer

View

System view

Default Level

2: System level

Parameters

interval-time: Interval (in minutes) to collect topology information, in the range 0 to 65,535. The value 0 means not to collect topology information.

Description

Use the **ntdp timer** command to configure the interval to collect topology information.

Use the **undo ntdp timer** command to restore the default.

By default, the interval to collect topology information is 1 minute.

Note that the management device can start to collect the topology information only after the cluster is set up.

Examples

Set the interval to collect the topology information to 30 minutes.

```
<Sysname> system-view
[Sysname] ntdp timer 30
```

ntdp timer hop-delay

Syntax

ntdp timer hop-delay *time*

undo ntdp timer hop-delay

View

System view

Default Level

2: System level

Parameters

time: Delay time (in milliseconds) for a device receiving topology-collection requests to forward them through its first port. This argument ranges from 1 to 1,000.

Description

Use the **ntdp timer hop-delay** command to set the delay time for the device to forward topology-collection requests through the first port.

Use the **undo ntdp timer hop-delay** command to restore the default delay time, which is 200 ms.

Examples

Set the delay time for the device to forward topology-collection requests through the first port to 300 ms.

```
<Sysname> system-view
[Sysname] ntdp timer hop-delay 300
```

ntdp timer port-delay

Syntax

ntdp timer port-delay *time*

undo ntdp timer port-delay

View

System view

Default Level

2: System level

Parameters

time: Delay time (in milliseconds) for a device to forward a topology-collection request through its successive ports, in the range 1 to 100.

Description

Use the **ntdp timer port-delay** command to set the delay time for a device to forward a received topology-collection request through its successive ports.

Use the **undo ntdp timer port-delay** command to restore the default delay time, or 20 ms.

Examples

Set the delay time for the device to forward topology-collection requests through the successive ports to 40 ms.

```
<Sysname> system-view
[Sysname] ntdp timer port-delay 40
```

Cluster Configuration Commands

add-member

Syntax

add-member [*member-number*] **mac-address** *mac-address* [**password** *password*]

View

Cluster view

Default Level

2: System level

Parameters

member-number: Member number assigned to the candidate device to be added to a cluster, ranging from 1 to 31.

mac-address: MAC address of the candidate device (in hexadecimal form of H-H-H).

password: Password of the candidate device, a string of 1 to 16 characters. The password is required when you add a candidate device to a cluster. However, this argument is not needed if the candidate device is not configured with a super password.

Description

Use the **add-member** command to add a candidate device to a cluster.

Note that:

- You must add a cluster member through the management device.
- When adding a member device to a cluster, you need not assign a number to the device. The management device will automatically assign a usable number to the newly added member device.
- After a candidate device joins the cluster, its level 3 password is replaced by the super password of the management device in cipher text.

Examples

Add a candidate device to the cluster, setting the member number to 6. (Assume that the MAC address and user password of the candidate device are 000f-e200-35E7 and 123456 respectively.)

```
<aabbcc_0.Sysname> system-view
[aabbcc_0.Sysname] cluster
[aabbcc_0.Sysname-cluster] add-member 6 mac-address 000f-e200-35e7 password 123456
```

administrator-address

Syntax

administrator-address *mac-address* **name** *cluster-name*

undo administrator-address

View

Cluster view

Default Level

2: System level

Parameters

mac-address: MAC address of the management device (in hexadecimal form of H-H-H).

cluster-name: Name of an existing cluster, a string of 1 to 8 characters, which can only be letters, numbers, subtraction sign (-), and underline (_).

Description

Use the **administrator-address** command to add a candidate device to a cluster.

Use the **undo administrator-address** command to remove a member device from the cluster.

By default, a device belongs to no cluster.

Note that:

- The **administrator-address** command is applicable on candidate devices only, while the **undo administrator-address** command is applicable on member devices only.
- You are recommended to use the **delete-member** command on the management device to remove a cluster member from a cluster.

Examples

Remove a member device from the cluster.

```
<aabbcc_1.Sysname> system-view
[aabbcc_1.Sysname] cluster
[aabbcc_1.Sysname-cluster] undo administrator-address
```

auto-build

Syntax

auto-build [**recover**]

View

Cluster view

Default Level

2: System level

Parameters

recover: Automatically reestablishes communication with all the member devices.

Description

Use the **auto-build** command to establish a cluster automatically.

Note that:

- This command can be executed on a candidate device or the management device.
- If you execute this command on a candidate device, you will be required to enter the cluster name to build a cluster. Then the system will collect candidates and add the collected candidates into the cluster automatically.
- If you execute this command on the management device, the system will collect candidates directly and add them into the cluster automatically.
- The **recover** keyword is used to recover a cluster. Using the **auto-build recover** command, you can find the members that are currently not in the member list and add them to the cluster again.

- Ensure that NTDP is enabled, because it is the basis of candidate and member collection. The collection range is also decided through NTDP. You can use the **ntdp hop** command in system view to modify the collection range.
- If a member is configured with a super password different from the super password of the management device, it cannot be added to the cluster automatically.

Examples

Establish a cluster automatically.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] auto-build
There is no base topology, if set up from local flash file?(Y/N)
y
  Begin get base topology file from local flash......
  Get file error, can not finish base topology recover

 Please input cluster name:aabbcc
 Collecting candidate list, please wait...

#Jul 22 14:35:18:841 2006 Sysname CLST/5/Cluster_Trap:
OID:1.3.6.1.4.1.2011.6.7.1.0.3: member 0.0.0.0.0.224.252.0.0.0 role change, NTDP
Index:0.0.0.0.0.0.224.252.0.0.0, Role:1
 Candidate list:

 Name                       Hops  MAC Address    Device

 Processing...please wait
 Cluster auto-build Finish!
 0 member(s) added successfully.
```

black-list add-mac

Syntax

black-list add-mac *mac-address*

View

Cluster view

Default Level

2: System level

Parameters

mac-address: MAC address of the device to be added into the blacklist, in the form of H-H-H.

Description

Use the **black-list add-mac** command to add a device to the blacklist.

Note that this command can be executed on the management device only.

Examples

Add a device with the MAC address of 0ec0-fc00-0001 to the blacklist.

```
<aabbcc_0.Sysname> system-view
[aabbcc_0.Sysname] cluster
[aabbcc_0.Sysname-cluster] black-list add-mac 0ec0-fc00-0001
```

black-list delete-mac

Syntax

black-list delete-mac { **all** | *mac-address* }

View

Cluster view

Default Level

2: System level

Parameters

all: Deletes all devices from the blacklist.

mac-address: MAC address of the device to be deleted from the blacklist, in the form of H-H-H.

Description

Use the **black-list delete-mac** command to delete a device from the blacklist.

Note that this command can be executed on the management device only.

Examples

Delete a device with the MAC address of 0EC0-FC00-0001 from the blacklist.

```
<aabbcc_0.Sysname> system-view
[aabbcc_0.Sysname] cluster
[aabbcc_0.Sysname-cluster] black-list delete-mac 0ec0-fc00-0001
```

Delete all devices in the blacklist.

```
[aabbcc_0.Sysname-cluster] black-list delete-mac all
```

build

Syntax

build *name*

undo build

View

Cluster view

Default Level

2: System level

Parameters

name: Cluster name, a string of 1 to 8 characters, which can only be letters, numbers, subtraction sign (-), and underline (_).

Description

Use the **build** command to configure the current device as the management device and specify a name for it.

Use the **undo build** command to configure the current management device as a candidate device.

By default, the device is not a management device.

Note that:

- When executing this command, you will be asked whether to create a standard topology map or not.
- This command can only be applied to devices that are capable of being a management device and are not members of other clusters. The command takes no effect if you execute the command on a device which is already a member of another cluster. If you execute this command on a management device, you will replace the cluster name with the one you specify.
- The member number of the management device is 0.

Examples

Configure the current device as a management device and specify the cluster name as **aabbcc**.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] build aabbcc
[Sysname-cluster] ip-pool 172.16.0.1 255.255.255.248
Restore topology from local flash file,for there is no base topology.
(Please confirm in 30 seconds, default No). (Y/N)
Y
  Begin get base topology file from local flash......
  Get file error, can not finish base topology recover

#Sep 18 19:56:03:804 2006 Sysname IFNET/4/INTERFACE UPDOWN:
 Trap 1.3.6.1.6.3.1.1.5.4: Interface 3276899 is Up, ifAdminStatus is 1, ifOperSt
atus is 1
#Sep 18 19:56:03:804 2006 Sysname CLST/4/Cluster_Trap:
OID:1.3.6.1.4.1.2011.6.7.1.0.3: member 0.0.0.0.0.224.252.0.29.0 role change, NTD
PIndex:0.0.0.0.0.0.224.252.0.29.0, Role:1
%Sep 18 19:56:03:804 2006 Sysname IFNET/4/UPDOWN:
 Line protocol on the interface Vlan-interface100 is UP
[aabbcc_0.Sysname-cluster]
%Sep 18 19:56:18:782 2006 Sysname CLST/4/LOG:
Member 000f-e200-1e00 is joined in cluster aabbcc.
[aabbcc_0.Sysname-cluster]
```

cluster

Syntax

cluster

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **cluster** command to enter cluster view.

Examples

Enter cluster view

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster]
```

cluster enable

Syntax

cluster enable

undo cluster enable

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **cluster enable** command to enable the cluster function.

Use the **undo cluster enable** command to disable the cluster function.

By default, the cluster function is enabled.

Note that:

- When you execute the **undo cluster enable** command on a management device, you remove the cluster and its members, and the device stops operating as a management device.

- When you execute the **undo cluster enable** command on a member device, you disable the cluster function on the device, and the device leaves the cluster.
- When you execute the **undo cluster enable** command on a device that belongs to no cluster, you disable the cluster function on the device.

Examples

Enable the cluster function.

```
<Sysname> system-view
[Sysname] cluster enable
```

cluster switch-to

Syntax

cluster switch-to { *member-number* | **mac-address** *mac-address* | **administrator** | **sysname** *member-sysname* }

View

User view

Default Level

0: Visit level

Parameters

member-number: Number of a member device in a cluster, in the range 1 to 31.

mac-address *mac-address*: MAC address of a member device, in the format of H-H-H.

administrator: Switches from a member device to the management device.

sysname *member-sysname*: System name of a member device, a string of 1 to 32 characters.

Description

Use the **cluster switch-to** command to switch between the management device and member devices.

Examples

Switch from the operation interface of the management device to that of the member device numbered 6 and then switch back to the operation interface of the management device.

```
<aaa_0.Sysname> cluster switch-to 6
<aaa_6.Sysname> quit
<aaa_0.Sysname>
```

Enter the member device numbered 5 with the system name of **switcha**.

```
<aaa_0.Sysname> cluster switch-to sysname switcha
SN    Device            MAC Address    Status Name
 5    Switch 4200G       000f-e200-5101  UP     test_5.switch
 6    Switch 4200G       000f-e200-5102  UP     test_6.switch
  press SN number to switch to the device, other number will quit the command:  5
<aaa_5.switcha>
```

cluster-local-user

Syntax

cluster-local-user *username* **password** { **cipher** | **simple** } *password*

undo cluster-local-user *username*

View

Cluster view

Default Level

1: Monitor level

Parameters

cipher: Indicates that the password is in cipher text.

simple: Indicates that the password is in plain text.

username: Username used for logging onto the devices within a cluster through Web, a string of 1 to 55 characters.

password: Password used for logging onto the devices within a cluster through Web. This password is a string of 1 to 63 characters when the **simple** keyword is specified, and can be in either plain text or cipher text when the **cipher** keyword is specified. A plain text password must be a string of 1 to 63 characters. The cipher text password must have a fixed length of 24 or 88 characters. The password is case sensitive.

Description

Use the **cluster-local-user** command to configure Web user accounts in batches.

Use the **undo cluster-local-user** command to remove the configuration.

Note that the command can be configured once on the management device only.

Examples

Configure Web user accounts for the devices within a cluster, with username being **abc**, password being 123456 and displayed in plain text.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-local-user abc password simple 123456
```

cluster-mac

Syntax

cluster-mac *mac-address*

undo cluster-mac

View

Cluster view

Default Level

2: System level

Parameters

mac-address: Multicast MAC address (in hexadecimal in the format of H-H-H), which can be 0180-c200-0000, 0180-c200-000a, 0180-c200-0020 through 0180-c200-002f, or 010f-e200-0002.

Description

Use the **cluster-mac** command to configure the destination MAC address for cluster management protocol packets.

Use the **undo cluster-mac** command to restore the default.

By default, the destination MAC address is 0180-c200-000a.

Note that this command can be executed on the management device only.

Examples

Set the multicast MAC address of the cluster management protocol packets to 0180-c200-0000.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] cluster-mac 0180-c200-0000
```

cluster-mac syn-interval

Syntax

cluster-mac syn-interval *interval-time*

View

Cluster view

Default Level

2: System level

Parameters

interval-time: Interval (in minutes) to send broadcast packets, in the range 0 to 30. If the interval is set to 0, the management device does not send broadcast packets to the member devices.

Description

Use the **cluster-mac syn-interval** command to set the interval for a management device to send MAC address negotiation broadcast packets for cluster management.

By default, the interval is set to one minute.

Note that this command can be executed on the management device only.

Examples

Set the interval for the management device to send MAC address negotiation broadcast packets for cluster management to two minutes.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] cluster-mac syn-interval 2
```

cluster-snmp-agent community

Syntax

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

undo cluster-snmp-agent community *community-name*

View

Cluster view

Default Level

1: Monitor level

Parameters

read: Indicates to allow the community's read-only access to MIB objects. The community with read-only authority can only query the device information.

write: Indicates to allow the community's read-write access to MIB objects. The community with read-write authority can configure the device information.

community-name: Community name, a string of 1 to 26 characters.

view-name: MIB view name, a string of 1 to 32 characters.

Description

Use the **cluster-snmp-agent community** command to configure an SNMP community shared by a cluster and set its access authority.

Use the **undo cluster-snmp-agent community** command to remove a specified community name.

Note that:

- The command used to configure the SNMP community with read or read-only authority can only be executed once on the management device. This configuration will be synchronized to the member devices in the whitelist, which is equal to configuring multiple member devices at one time.
- SNMP community name will be retained if a cluster is dismissed or a member device is removed from the whitelist.
- If the same community name as the current one has been configured on a member device, the current community name will replace the original one.

Examples

Configure the SNMP community name shared by a cluster as **comaccess** and allow the community's read-only access to MIB objects.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent community read comaccess
```

Configure the SNMP community name shared by a cluster as **comaccesswr** and allow the community's read-write access to MIB objects.

```
[aaa_0.Sysname-cluster] cluster-snmp-agent community write comacceswr
```

cluster-snmp-agent group v3

Syntax

cluster-snmp-agent group v3 *group-name* [**authentication | privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*]

undo cluster-snmp-agent group v3 *group-name* [**authentication | privacy**]

View

Cluster view

Default Level

1: Monitor level

Parameters

group-name: Group name, a string of 1 to 32 characters.

authentication: Specifies to authenticate a packet but not to encrypt it.

privacy: Specifies to authenticate and encrypt a packet.

read-view: Read-only view name, a string of 1 to 32 characters.

write-view: Read-write view name, a string of 1 to 32 characters.

notify-view: View name in which Trap messages can be sent, a string of 1 to 32 characters.

Description

Use the **cluster-snmp-agent group** command to configure the SNMPv3 group shared by a cluster and set its access rights.

Use the **undo cluster-snmp-agent group** command to remove the SNMPv3 group shared by a cluster.

Note that:

- The command can be executed once on the management device only. This configuration will be synchronized to the member devices in the whitelist, which is equal to configuring multiple member devices at one time.
- SNMPv3 group name will be retained if a cluster is dismissed or a member device is deleted from the whitelist.
- If the same group name as the current one has been configured on a member device, the current group name will replace the original one.

Examples

Create an SNMP group **snmpgroup**.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent group v3 snmpgroup
```

cluster-snmp-agent mib-view included

Syntax

cluster-snmp-agent mib-view included *view-name oid-tree*

undo cluster-snmp-agent mib-view *view-name*

View

Cluster view

Default Level

1: Monitor level

Parameters

view-name: MIB view name, a string of 1 to 32 characters.

oid-tree: MIB subtree, a string of 1 to 255 characters, which can only be a variable OID string or variable name string. OID is composed of a series of integers, indicating where a node is in the MIB tree. It can uniquely identify an object in a MIB.

Description

Use the **cluster-snmp-agent mib-view included** command to create or update the MIB view information shared by a cluster.

Use the **undo cluster-snmp-agent mib-view** command to delete the MIB view information shared by a cluster.

By default, the MIB view name shared by a cluster is ViewDefault, in which the cluster can access ISO subtree.

Note that:

- This command can be executed once on the management device only. This configuration will be synchronized to member devices on the whitelist, which is equal to configuring multiple member devices at one time.
- The MIB view will be retained if a cluster is dismissed or a member device is deleted from the whitelist.
- If the same view name as the current one has been configured on a member device, the current view will replace the original one on the member device.

Examples

Create a view including all objects of **mib2**.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent mib-view included mib2 1.3.6.1.2.1
```

cluster-snmp-agent usm-user v3

Syntax

cluster-snmp-agent usm-user v3 *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password*] [**privacy-mode des56** *priv-password*]

undo cluster-snmp-agent usm-user v3 *user-name group-name*

View

Cluster view

Default Level

1: Monitor level

Parameters

user-name: User name, a string of 1 to 32 characters.

group-name: Group name, a string of 1 to 32 characters.

authentication-mode: Specifies the security level to be authentication needed.

md5: Specifies the authentication protocol to be HMAC-MD5-96.

sha: Specifies the authentication protocol to be HMAC-SHA-96.

auth-password: Authentication password, a string of 1 to 16 characters if in plain text; it can only be a string of 24 characters if in cipher text.

privacy-mode: Specifies the security level to be encrypted.

des56: Specifies the encryption protocol to be DES (data encryption standard).

priv-password: Encryption password, a string of 1 to 16 characters in plain text; it can only be a string of 24 characters in cipher text.

Description

Use the **cluster-snmp-agent usm-user v3** command to add a new user to the SNMP v3 group shared by a cluster.

Use the **undo cluster-snmp-agent usm-user v3** command to delete the SNMP v3 group user shared by the cluster.

Note that:

- The command can be executed once on the management device only. This configuration will be synchronized to member devices on the whitelist, which is equal to configuring multiple member devices at one time.
- SNMPv3 group user will be retained if a cluster is dismissed or a member device is deleted from the whitelist.
- If the same username as the current one has been configured on a member device, the current username will replace the original one on the member device.

Examples

Add a user **wang** to the SNMP group **snmpgroup**, set the security level to authentication-needed and specify the authentication protocol as HMAC-MD5-96 and authentication password as **pass**.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] cluster-snmp-agent usm-user v3 wang snmpgroup authentication-mode
md5 pass
```

delete-member

Syntax

delete-member *member-number* [**to-black-list**]

View

Cluster view

Default Level

2: System level

Parameters

member-number: Number of a member device in a cluster, in the range 1 to 31.

to-black-list: Adds the device removed from a cluster to the blacklist to prevent it from being added to the cluster.

Description

Use the **delete-member** command to remove a member device from the cluster.

Note that you should perform the operation to remove a member device from a cluster on the management device only.

Examples

Remove the member device numbered 2 from the cluster.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] delete-member 2
```

Remove the member device numbered 3 from the cluster, and add it to the blacklist.

```
[aaa_0.Sysname-cluster] delete-member 3 to-black-list
```

display cluster

Syntax

display cluster

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display cluster** command to display the state and statistics of the cluster to which the current device belongs.

Note that this command can be executed on the management device and member devices only.

Examples

Display cluster information on the management device.

```
<aaa_0.Sysname> display cluster
Cluster name:"aaa"
 Role:Administrator
 Management-vlan:100
 Handshake timer:10 sec
 Handshake hold-time:60 sec
 IP-Pool:1.1.1.1/16
 cluster-mac:0180-c200-000a
 No logging host configured
 No SNMP host configured
 No FTP server configured
 No TFTP server configured

 2 member(s) in the cluster, and 0 of them down.
```

Display cluster information on a member device.

```
<aaa_1.Sysname> display cluster
Cluster name:"aaa"
 Role:Member
 Member number:1
 Management-vlan:100
 cluster-mac:0180-c200-000a
 Handshake timer:10 sec
 Handshake hold-time:60 sec

 Administrator device IP  address:1.1.1.1
 Administrator device mac address:000f-e200-1d00
 Administrator status:Up
```

Table 20-5 display cluster command output description

Field	Description
Cluster name	Name of the cluster
Role	Role of the switch in the cluster, Administrator means the current device is a management device and Member means the current device is a member device.
Member number	Member number of the switch in the cluster
Management-vlan	Management VLAN of the cluster
Handshake timer	Interval to send handshake packets
Handshake hold-time	Value of handshake timer

Field	Description
IP-Pool	Private IP addresses of the member devices in the cluster
cluster-mac	Multicast MAC address of cluster management packets
Administrator device IP address	IP address of the management device
Administrator device mac address	MAC address of the management device
Administrator status	State of the management device

display cluster base-topology

Syntax

display cluster base-topology [**mac-address** *mac-address* | **member-id** *member-number*]

View

Any view

Default Level

2: System level

Parameters

mac-address: Specifies a device by its MAC address. The system will display the standard topology with the device as the root.

member-number: Specifies a device by its number. The system will display the standard topology with the device as the root.

Description

Use the **display cluster topology** command to display the standard topology of a cluster.

You can create a standard topology map when executing the **build** or **auto-build** command, or you can use the **topology accept** command to save the current topology map as the standard topology map.

Note that this command can be executed on the management device only.

Examples

Display the standard topology of a cluster.

```
<aaa_0.Sysname> display cluster base-topology
-------------------------------------------------------------------------
    (PeerPort) ConnectFlag (NativePort) [SysName:DeviceMac]
-------------------------------------------------------------------------
[aaa_0.Sysname:000f-e200-1400]
    |
    ├-(P_4/1)<-->(P_1/7)[Sysname:000f-e200-3333]
    |   |
    |   ├-(P_1/7)<-->(P_4/1)[aaa_3.Sysname:000f-e200-0000]
    |   |   |
    |   |   ├-(P_4/1)<-->(P_4/1)[aaa_0.Sysname:000f-e200-1400]
```

```
|   |   |
|   |   ├-(P_4/1)<-->(P_1/9)[Sysname:000f-e200-4510]
|   |   |
|   |   └-(P_4/1)<-->(P_1/11)[Sysname:000f-e200-7000]
|   |
|   ├-(P_1/7)<-->(P_1/9)[Sysname:000f-e200-4510]
|   |   |
|   |   ├-(P_1/9)<-->(P_4/1)[aaa_0.3Com:000f-e200-1400]
|   |   |
|   |   └-(P_1/9)<-->(P_1/11)[Sysname:000f-e200-7000]
|   |
|   └-(P_1/7)<-->(P_1/11)[Sysname:000f-e200-7000]
|       |
|       ├-(P_1/3)<-->(P_1/2)[aaa_2.Sysname:00e0-fd00-4510]
|       |
|       ├-(P_1/10)<-->(P_4/1)[Sysname:000f-e205-4300]
|       |
|       ├-(P_1/11)<-->(P_4/1)[aaa_0.Sysname:000f-e200-1400]
|       |
|       └-(P_1/8)<-->(P_1/12)[aaa_1.Sysname:000f-e200-7016]
|
├-(P_4/1)<-->(P_4/1)[aaa_3.Sysname:000f-e200-0000]
|   |
|   ├-(P_4/1)<-->(P_1/9)[Sysname:000f-e200-4510]
|   |
|   └-(P_4/1)<-->(P_1/11)[Sysname:000f-e200-7000]
|
├-(P_4/1)<-->(P_1/9)[Sysname:000f-e200-4510]
|   |
|   └-(P_1/9)<-->(P_1/11)[Sysname:000f-e200-7000]
|
└-(P_4/1)<-->(P_1/11)[Sysname:000f-e200-7000]
    |
    ├-(P_1/3)<-->(P_1/2)[aaa_2.Sysname:00e0-fd00-4510]
    |
    ├-(P_1/10)<-->(P_4/1)[Sysname:000f-e205-4300]
    |
    └-(P_1/8)<-->(P_1/12)[aaa_1.Sysname:000f-e200-7016]
```

Table 20-6 display cluster base-topology command output description

Field	Description
PeerPort	Peer port
ConnectFlag	Connection flag: <-->
NativePort	Local port
SysName	System name of the peer device
DeviceMac	MAC address of the peer device

display cluster black-list

Syntax

display cluster black-list

View

Any view

Default Level

2: System level

Parameters

None

Description

Use the **display cluster black-list** command to display the current blacklist of a cluster.

Note that this command can be executed on the management device only.

Examples

View the current blacklist of the cluster.

```
<aaa_0.Sysname> display cluster black-list
  Device ID          Access Device ID          Access port
  000f-e200-0010     000f-e200-3550            GigabitEthernet1/0/1
```

Table 20-7 display cluster black-list command output description

Field	Description
Device ID	ID of the blacklist device, indicated by its MAC address.
Access Device ID	ID of the device connected to the blacklist device, indicated by its MAC address.
Access port	Port connected to the blacklist device.

display cluster candidates

Syntax

display cluster candidates [**mac-address** *mac-address* | **verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

mac-address *mac-address*: Specifies the MAC address of a candidate device, in the format of H-H-H.

verbose: Displays the detailed information about a candidate device.

Description

Use the **display cluster candidates** command to display the information about the candidate devices of a cluster.

Note that the command can be executed on the management device only.

Examples

Display the information about all the candidate devices.

```
<aaa_0.Sysname> display cluster candidates
 MAC           HOP  IP               Device
 000f-e200-3199  3                    Switch 4200G
 000f-cbb8-9528  1    31.31.31.56/24     Switch 4200G
```

Table 20-8 display cluster candidates command output description

Field	Description
MAC	MAC address of a candidate device
HOP	Hops from a candidate device to the management device
IP	IP address of a candidate device
Device	Platform information of a device

Display the information about a specified candidate device.

```
<aaa_0.Sysname> display cluster candidates mac-address 000f-e261-c4c0
Hostname  : LSW1
 MAC      : 000f-e261-c4c0
 Hop      : 1
 Device    : Sysname Switch 4200G
 IP       : 1.5.6.9/16
```

Display the detailed information about all the candidate devices.

```
<aaa_0.Sysname> display cluster candidates verbose
 Hostname  : 3100_4
 MAC      : 000f-e200-3199
 Hop      : 3
 Device  : Switch 4200G
 IP       :

 Hostname  : Sysname
 MAC      : 000f-cbb8-9528
 Hop      : 1
 Device  : Switch 4200G
 IP       : 31.31.31.56/24
```

Table 20-9 display cluster candidates verbose command output description

Field	Description
Hostname	Name of a candidate device
MAC	MAC address of a candidate device
Hop	Hops from a candidate device to the management device
IP	IP address of a candidate device
Device	Platform information of a candidate device

display cluster current-topology

Syntax

display cluster current-topology [**mac-address** *mac-address* [**to-mac-address** *mac-address*] | **member-id** *member-number* [**to-member-id** *member-number*]]

View

Any view

Default Level

2: System level

Parameters

member-number: Number of the devices in a cluster (including the management device and member devices).

mac-address: MAC addresses of the devices in a cluster (including the management device and member devices).

Description

Use the **display cluster current-topology** command to display the current topology information of the cluster.

- If you specify both the **mac-address** *mac-address* and **to-mac-address** *mac-address* arguments, the topology information of the devices that are in a cluster and form the connection between two specified devices is displayed.
- If you specify both the **member-id** *member-number* and **to-member-id** *member-number* arguments, the topology information of the devices that are in a cluster and form the connection between two specified devices is displayed.
- If you specify only the **mac-address** *mac-address* or **member-id** *member-number* argument, the topology information of all the devices in a cluster is displayed, with a specified device as the root node.

Note that this command can be executed on the management device only.

Examples

Display the information of the current topology of a cluster.

```
<aaa_0.Sysname> display cluster current-topology
```

```
------------------------------------------------------------------------
    (PeerPort) ConnectFlag (NativePort) [SysName:DeviceMac]
------------------------------------------------------------------------
ConnectFlag:
    <--> normal connect     ---> odd connect     **** in blacklist
    ???? lost device        ++++ new device      -||- STP discarding
------------------------------------------------------------------------
[aaa_0.Sysname:000f-e200-7016]
   |
   └-(P_1/12)++++(P_1/8)[Sysname:000f-e200-7000]
       |
       |-(P_1/11)++++(P_1/9)[Sysname:000f-e200-4510]
       |   |
       |   |-(P_1/9)++++(P_4/1)[aaa_2.Sysname:000f-e200-0000]
       |   |
       |   └-(P_1/9)++++(P_1/7)[Sysname:000f-e200-3333]
       |
       |-(P_1/11)++++(P_4/1)[bbb_2.3Com:000f-e200-0000]
       |   |
       |   └-(P_4/1)++++(P_1/7)[Sysname:000f-e200-3333]
       |
       └-(P_1/11)++++(P_1/7)[Sysname:000f-e200-3333]
```

Table 20-10 display cluster current-topology command output description

Field	Description
PeerPort	Peer port
ConnectFlag	Connection flag
NativePort	Local port
SysName:DeviceMac	System name of the device
<--> normal connect	Indicates a normal connection between the device and the management device
---> odd connect	Indicates a unidirectional connection between the device and the management device
**** in blacklist	Indicates the device is in the blacklist
???? lost device	Indicates a lost connection between the device and the management device
++++ new device	Indicates this is a new device, whose identity is to be recognized by the administrator
-||- STP discarding	STP is blocked

Note

A new device in the topology information is identified based on the standard topology. After you add a device into a cluster, if you do not use the **topology accept** command to confirm the current topology and save it as the standard topology, this device is still regarded as a new device.

display cluster members

Syntax

display cluster members [*member-number* | **verbose**]

View

Any view

Default Level

1: Monitor level

Parameters

member-number: Number of the member device, in the range 0 to 31.

verbose: Displays the detailed information about all the devices in a cluster.

Description

Use the **display cluster members** command to display the information about cluster members.

Note that this command can be executed on the management device only.

Examples

Display the information about all the devices in a cluster.

```
<aaa_0.Sysname> display cluster members
 SN   Device            MAC Address     Status Name
 0    Switch 4200G       000f-e200-1751  Admin  123_0.3100_1
 2    Switch 4200G       000f-e200-3199  Up     123_2.3100_4
 3    Sysname S3628P     00e0-fd00-0043  Up     123_3.S3528P
 4    Switch 4200G       00f-e200-2579   Up     123_4.3100_2
 5    Switch 4200G       000f-e20f-c415  Up     123_5.3100_5
```

Table 20-11 display cluster members command output description

Field	Description
SN	Member number
Device	Device type
MAC Address	MAC address of a device

Field	Description
Status	State of a device: • *up: The member device which is up* • *down: The member which is down* • *deleting: The member which is being deleted* • *admin: The management device*
Name	Name of a device

Display the detailed information about the management device and all member devices.

```
<aaa_0.Sysname> display cluster members verbose
 Member number:0
 Name:aaa_0.Sysname
 Device:Switch 4210G PWR 48-Port
 MAC Address:000f-e2d2-58fb
 Member status:Admin
 Hops to administrator device:0
 IP: 192.168.0.88/24
 Version:
  3Com Corporation
  3Com OS Software Version 5.20 Release 2202P17 Release 2202P17
  Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved.
  Switch 4210G PWR 48-Port V300R001B01D021


 Member number:2
 Name:aaa_2.Sysname
 Device:3Com S7902E
 MAC Address:000f-e234-5678
 Member status:Up
 Hops to administrator device:2
 IP: 192.168.0.71/24
 Version:
  3Com Corporation
  3Com OS Software Version 3ComComware Release 520 Test 6610
  Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved.
  3Com S7902E V600R006B02D076SP03, Test 6610


 Member number:3
 Name:aaa_3.Sysname
 Device:Switch 4210G 24-Port
 MAC Address:00e0-fc00-5502
 Member status:Up
 Hops to administrator device:2
 IP: 192.168.0.86/24
 Version:
  3Com Corporation
```

```
3Com OS Software Version 5.20 Release 2202P17 Release 2202P17
Copyright (c) 2004-2009 3Com Corp. and its licensors. All rights reserved.
Switch 4210G 24-Port V300R001B01D021
```

Table 20-12 display cluster members verbose command output description

Field	Description
Member number	Device member number
Name	Name of a member device, composed of the cluster name and the host name of the member device, in the format of cluster name.hostname When the management device type is not consistent with the member device type, if a user modifies the cluster name on the management device continuously, the cluster name may appear twice in the cluster member name, for example, “clustername.clustername.hostname”. This abnormal case can restore in a period of time.
Device	Device type
MAC Address	MAC address of a device
Member status	State of a device
Hops to administrator device	Hops from the current device to the management device
IP	IP address of a device
Version	Software version of the current device

ftp-server

Syntax

ftp-server *ip-address* [**user-name** *username* **password** { **simple** | **cipher** } *password*]

undo ftp-server

View

Cluster view

Default Level

3: Manage level

Parameters

ip-address: IP address of the FTP server.

username: Username used to log onto the FTP server, a string of 1 to 32 characters.

simple: Indicates that the password is in plain text.

cipher: Indicates that the password is in cipher text.

password: Password used to log onto the FTP server. This password must be in plain text when the **simple** keyword is specified, and can be in either plain text or cipher text when the **cipher** keyword is specified. A plain text password must be a string of no more than 16 characters, such as “aabbcc”. The cipher text password must have a fixed length of 24 characters, such as _(TT8F]Y\5SQ=^Q`MAF4<1!!.

Description

Use the **ftp-server** command to configure a public FTP server (by setting its IP address, username, and password) on the management device for the member devices in the cluster.

Use the **undo ftp-server** command to remove the FTP server configured for the member devices in the cluster.

By default, a cluster is not configured with a public FTP server.

Note that the command can be executed on the management device only.

Examples

Set the IP address, username and password of an FTP server shared by the cluster on the management device to be 1.0.0.9, **ftp**, and in plain text respectively.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] ftp-server 1.0.0.9 user-name ftp password simple ftp
```

holdtime

Syntax

holdtime *seconds*

undo holdtime

View

Cluster view

Default Level

2: System level

Parameters

seconds: Holdtime in seconds, in the range 1 to 255.

Description

Use the **holdtime** command to configure the holdtime of a device.

Use the **undo holdtime** command to restore the default.

By default, the holdtime of a device is 60 seconds.

Note that this command can be executed on the management device only. The configuration is valid on all member devices in a cluster.

Examples

Set the holdtime to 30 seconds.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
```

```
[aaa_0.Sysname-cluster] holdtime 30
```

ip-pool

Syntax

ip-pool *administrator-ip-address* { *mask* | *mask-length* }

undo ip-pool

View

Cluster view

Default Level

2: System level

Parameters

administrator-ip-address: Private IP address of the management device in a cluster.

mask | *mask-length*: Mask of the IP address pool of a cluster. It is an integer or in dotted decimal notation. When it is an integer, it ranges from 1 to 30. A network address can be obtained by ANDing this mask with *administrator-ip-addres*s. The private IP addresses of all member devices in a cluster belong to this network segment.

Description

Use the **ip-pool** command to configure a private IP address range for cluster members.

Use the **undo ip-pool** command to remove the IP address range configuration.

By default, no private IP address range is configured for cluster members.

Note that:

- You must configure the IP address range on the management device only and before establishing a cluster. If a cluster has already been established, you are not allowed to change the IP address range.
- For a cluster to work normally, the IP addresses of the VLAN interfaces of the management device and member devices must not be in the same network segment as that of the cluster address pool.

Examples

Configure the IP address range of a cluster.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.200.0.1 20
```

logging-host

Syntax

logging-host *ip-address*

undo logging-host

View

Cluster view

Default Level

2: System level

Parameters

ip-address: IP address of the logging host.

Description

Use the **logging-host** command to configure a logging host shared by a cluster.

Use the **undo logging-host** command to remove the logging host configuration.

By default, no logging host is configured for a cluster.

Note that:

- This command can be executed on the management device only.
- You have to execute the **info-center loghost** command in system view first for the logging host you configured to take effect.

For related configuration, refer to the **info-center loghost** command in *Information Center Commands* in the *System Volume*.

Examples

Configure the IP address of the logging host shared by a cluster on the management device as 10.10.10.9.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] logging-host 10.10.10.9
```

management-vlan

Syntax

management-vlan *vlan-id*

undo management-vlan

View

System view

Default Level

2: System level

Parameters

vlan-id: ID of the management VLAN, in the range 1 to 4094.

Description

Use the **management-vlan** command to specify the management VLAN.

Use the **undo management-vlan** command to restore the default.

By default, VLAN 1 is the management VLAN.

Note that:

- The management VLAN must be specified before a cluster is created. Once a member device is added to a cluster, the management VLAN configuration cannot be modified. To modify the management VLAN for a device belonging to a cluster, you need to cancel the cluster-related configurations on the device, specify the desired VLAN to be the management VLAN, and then re-create the cluster.
- For the purpose of security, you are not recommended to configure the management VLAN as the default VLAN ID of the port connecting the management device and the member devices.
- Only when the default VLAN ID of all cascade ports and the port connecting the management device and the member device is the management VLAN, can the packets in the management VLAN packets be passed without a tag. Otherwise, you must configure the packets from a management VLAN to pass these ports. For the configuration procedure, refer to *VLAN Configuration* in the *Access Volume*.

Examples

Specify VLAN 2 as the management VLAN.

```
<Sysname> system-view
[Sysname] management-vlan 2
```

management-vlan synchronization enable

Syntax

management-vlan synchronization enable

undo management-vlan synchronization enable

View

Cluster view

Default Level

1: Monitor level

Parameters

None

Description

Use the **management-vlan synchronization enable** command to enable the management VLAN auto-negotiation function.

Use the **undo management-vlan synchronization enable** command to disable the management VLAN auto-negotiation function.

By default, the management VLAN auto-negotiation function is disabled.

Examples

Enable the management VLAN auto-negotiation function on the management device.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] management-vlan synchronization enable
```

nm-interface vlan-interface

Syntax

nm-interface vlan-interface *vlan-interface-id*

View

Cluster view

Default Level

2: System level

Parameters

vlan-interface-id: ID of the VLAN interface. The value range is the same as that of the existing VLAN interface ID.

Description

Use the **nm-interface vlan-interface** command to configure the VLAN interface of the access management device (including FTP/TFTP server, management host and log host) as the network management interface of the management device.

Examples

Configure VLAN-interface 2 as the network management interface.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] nm-interface vlan-interface 2
```

reboot member

Syntax

reboot member { *member-number* | **mac-address** *mac-address* } [**eraseflash**]

View

Cluster view

Default Level

2: System level

Parameters

member-number: Number of the member device, in the range 1 to 31.

mac-address *mac-address*: MAC address of the member device to be rebooted, in the format of H-H-H.

eraseflash: Deletes the configuration file when the member device reboots.

Description

Use the **reboot member** command to reboot a specified member device on the management device.

Examples

Reboot the member device numbered 2.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] reboot member 2
```

snmp-host

Syntax

snmp-host *ip-address* [**community-string read** *string1* **write** *string2*]

undo snmp-host

View

Cluster view

Default Level

3: Manage level

Parameters

ip-address: IP address of an SNMP host.

string1: Community name of read-only access, a string of 1 to 26 characters.

string2: Community name of read-write access, a string of 1 to 26 characters.

Description

Use the **snmp-host** command to configure a shared SNMP host for a cluster.

Use the **undo snmp-host** command to cancel the SNMP host configuration.

By default, no SNMP host is configured for a cluster.

Note that this command can be executed on the management device only.

Examples

Configure a shared SNMP host for the cluster on the management device.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] snmp-host 1.0.0.9 community-string read 123 write 456
```

tftp-server

Syntax

tftp-server *ip-address*

undo tftp-server

View

Cluster view

Default Level

2: System level

Parameters

ip-address: IP address of a TFTP server.

Description

Use the **tftp-server** command to configure a shared TFTP server for a cluster.

Use the **undo tftp-server** command to cancel the TFTP server of the cluster.

By default, no TFTP server is configured.

Note that this command can be executed on the management device only.

Examples

Configure a shared TFTP server on the management device as 1.0.0.9.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] tftp-server 1.0.0.9
```

timer

Syntax

timer *interval-time*

undo timer

View

Cluster view

Default Level

2: System level

Parameters

interval-time: Interval (in seconds) to send handshake packets. This argument ranges from 1 to 255.

Description

Use the **timer** command to set the interval to send handshake packets.

Use the **undo timer** command to restore the default.

By default, the interval to send handshake packets is 10 seconds.

Note that this command can be executed on the management device only and is valid for all member devices in a cluster.

Examples

Configure the interval to send handshake packets as 3 seconds.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] timer 3
```

topology accept

Syntax

topology accept { **all** [**save-to** { **ftp-server** | **local-flash** }] | **mac-address** *mac-address* | **member-id** *member-number* }

undo topology accept { **all** | **mac-address** *mac-address* | **member-id** *member-number* }

View

Cluster view

Default Level

2: System level

Parameters

all: Accepts the current cluster topology information as the standard topology information.

mac-address *mac-address*: Specifies a device by its MAC address. The device will be accepted to join the standard topology of the cluster.

member-id *member-number*: Specifies a device by its member number. The device will be accepted to join the standard topology of the cluster. The *member-number* argument is in the range 0 to 31.

save-to: Confirms the current topology as the standard topology, and backs up the standard topology on the FTP server or local flash in a file named “topology.top”.

Description

Use the **topology accept** command to confirm the current topology information and save it as the standard topology.

Use the **undo topology accept** to delete the standard topology information.

Note that:

- This command can be executed on the management device only.
- The file used to save standard topology on the FTP server or the local flash is named “topology.top”, which includes both the information of blacklist and whitelist. A blacklist contains the devices that are prohibited to be added to a cluster. A whitelist contains devices that can be added to a cluster.

Examples

Take the current topology as the standard topology.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] topology accept all
```

topology restore-from

Syntax

topology restore-from { **ftp-server** | **local-flash** }

View

Cluster view

Default Level

2: System level

Parameters

ftp-server: Restores the standard topology information from the FTP server.

local-flash: Restores the standard topology information from the local flash.

Description

Use the **topology restore-from** command to restore the standard topology information from the FTP server or the local flash in case the cluster topology information is incorrect.

Note that:

- This command can be executed on the management device only.
- If the stored standard topology is not correct, the device cannot be aware of if. Therefore, you must ensure that the standard topology is correct.

Examples

Restore the standard topology.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] topology restore-from local-flash
```

topology save-to

Syntax

topology save-to { **ftp-server** | **local-flash** }

View

Cluster view

Default Level

2: System level

Parameters

ftp-server: Saves the standard topology information to the FTP server.

local-flash: Saves the standard topology information to the local flash.

Description

Use the **topology save-to** command to save the standard topology information to the FTP server or the local flash.

Note that:

- The file used to save standard topology on the FTP server or the local flash is named “topology.top”, which includes both the information of blacklist and whitelist. A blacklist contains the devices that are prohibited to be added to a cluster. A whitelist contains devices that can be added to a cluster.
- This command can be executed on the management device only.

Examples

Save the standard topology information to the local flash.

```
<Sysname> system-view
[Sysname] cluster
[Sysname-cluster] ip-pool 10.1.1.1 24
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster] topology save-to local-flash
```

21 IRF Configuration Commands

Note

Among Switch 4210G series switches, Switch 4210G 24-Port, Switch 4210G 48-Port, Switch 4210G PWR 24-Port, and Switch 4210G PWR 48-Port switches support IRF.

IRF Configuration Commands

display irf

Syntax

display irf

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display irf** command to display the information of the current Intelligent Resilient Framework (IRF) , which has the device you are working on as its IRF member.

The command displays the information of IRF members, and the information of the devices that are joining in this IRF.

Examples

Display the information of the current IRF.

```
<Sysname> display irf
Switch     Role        Priority      CPU-MAC
    1      Slave       13            000f-e2b8-1f84
    2      Slave       1             000f-e220-2122
   *3      Master      20            000f-e2b8-1a82
   +4      SlaveWait   1             000f-e2c8-1b82
-------------------------------------------------------
 * indicates the device is the master.
```

```
 + indicates the device through which the user logs in.
The Bridge MAC of the IRF is : 000f-e2b8-1a61
Auto upgrade               : yes
Mac persistent             : 6 min
```

Table 21-1 display irf command output description

Field	Description
Switch	Member ID. • The ID with * indicates that the device is the master; • The ID with + indicates that it is the device through which the user logs in to the IRF.
Role	The role of a member in the IRF, which may take the following values: • Slave • Master • SlaveWait • Loading
CPU-MAC	CPU MAC address of the device
Auto upgrade	Whether the auto upgrade of configuration files is enabled: • yes: Enabled • no: Disabled
Mac persistent	Whether the IRF bridge MAC address preservation is enabled: • yes: Enabled • no: Disabled

display irf configuration

Syntax

display irf configuration

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display irf configuration** command to display the pre-configurations of IRF members in the current IRF.

The pre-configuration takes effect after the reboot of the device. The command displays the member ID, IRF port, and physical IRF port information.

Examples

Display the pre-configurations of all the IRF members in the current IRF.

```
<Sysname> display irf configuration
MemberID   NewID   IRF-Port1    IRF-Port2
   1         1       1,2           3,4
   2         2       1,2           3
  *3         3       1             3
  +4         4       1             disable
-------------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.
```

Table 21-2 display irf configuration command output description

Field	Description
MemberID	Member ID • The ID with * indicates that the device is the master; • The ID with + indicates that it is the device through which the users logs in to the IRF.
NewID	The member ID configured for a device after its reboot
IRF-Port1	The physical IRF port number corresponding to IRF port 1 of a device after its reboot. (If it displayed in the format of **x**, it indicates that IRF port 1 is bound to physical IRF port x; if it is displayed in the format of **x,y**, it indicates that IRF port 1 is aggregated by physical IRF ports x and y; if it is displayed as **disable**, it indicates that IRF port 1 is not enabled.)
IRF-Port2	The physical IRF port number corresponding to IRF port 2 of a device after its reboot. (If it displayed in the format of **x**, it indicates that IRF port 2 is bound to physical IRF port x; if it is displayed in the format of **x,y**, it indicates that IRF port 2 is aggregated by physical IRF ports x and y; if it is displayed as **disable**, it indicates that IRF port 2 is not enabled.)

display irf topology

Syntax

display irf topology

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display irf topology** command to display the topology information of the current IRF.

The command displays all the topology information learned by the current device.

Examples

Display the topology information of the current IRF.

```
<Sysname> display irf topology
                      Topology Info
------------------------------------------------------------------------
               IRF-Port1                IRF-Port2
 Switch   Link   member   neighbor   Link   member   neighbor  Belong To
   1      DOWN   1,2      --         UP     3,4      2         000f-cbb8-1a82
   2      UP     1,2      1          UP     3        3         000f-cbb8-1a82
 *+3      UP     1        2          DIS    --       --        000f-cbb8-1a82
------------------------------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.
```

The above information indicates following:

- On device 1, IRF port 1 is aggregated from physical IRF ports 1 and 2, and it is down; IRF port 2 is aggregated from physical IRF ports 3 and 4, and it is up.
- On device 2, IRF port 1 is aggregated from physical IRF ports 1 and 2, and it is up; IRF port 2 corresponds to physical IRF port 3, and it is up.
- On device 3, IRF port 1 corresponds to physical IRF port 1, and it is up; IRF is disabled on IRF port 2.
- IRF port 1 of device 1 does not connect with any other device; IRF port 2 of device 1 connects to IRF port 1 of device 2; IRF port 2 connects to IRF port 1 of device 3; IRF port 2 of device 3 does not connect with any other device.
- All the three devices belong to one IRF. The bridge MAC address of the master is 000f-cbb8-1a82.

Network topology view is as shown in Figure 21-1:

Figure 21-1 Network topology view

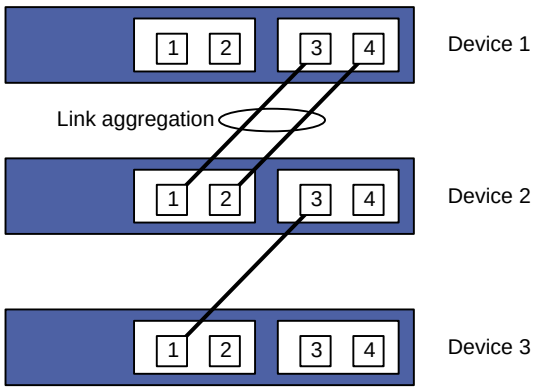

Table 21-3 display irf topology command output description

Field	Description
Switch	Member ID • The ID with * indicates that the device is the master; • The ID with + indicates that it is the device through which the users logs in to the IRF.
IRF-Port 1	Information of IRF port 1, including link (link state), member (corresponding physical port), and neighbor.
IRF-Port 2	Information of IRF port 2, including link, member, and neighbor.

Field	Description
BelongTo	The IRF that the device belongs to, represented by the IRF CPU MAC address.
Link	Link state of the IRF port: • UP • DOWN • ISOLATE: The corresponding physical IRF port is isolated because it cannot meet the requirement of the IRF. The reason may be that the physical IRF port connects to a non-Switch 4210G device, or the IRF port of the peer end is not connected according to the port serial numbers. • TIMEOUT: The port does not receive any Hello packet from the peer end after the expected time, that is, the Hello packet sent to the port times out. • DIS: The IRF port is not enabled.
member	The corresponding physical port(s) of the IRF port. If the IRF port is disabled, -- will be displayed.
neighbor	The device ID that connects with this IRF port If the IRF port does not connect with any device, -- will be displayed.

display switchover state

Syntax

display switchover state [**slot** *slot-id*]

View

Any view

Default Level

1: Monitor level

Parameters

slot *slot-id*: ID of the IRF member. With this argument, the command displays the master/slave switchover state of the specified IRF member. Without this argument, the command displays the master/slave switchover state of the IRF master.

Description

Use the **display switchover state** command to display the master/slave switchover states of IRF members.

An IRF functions like a logical distributed device with multiple standby switching and routing processing units (SRPUs). The master is like the active SRPU, and the slaves are like the standby SRPUs. An IRF system uses member ID to uniquely identify a member device, whereas a distributed device uses slot ID to uniquely identify a board. Therefore, in the displayed information of this command, a member device is also identified by the slot ID, which is equal to the member ID.

Examples

Display the master/slave switchover states of the master.

```
<Sysname> display switchover state
Master HA State to Slot [1]: Slave is absent.
Master HA State to Slot [2]: Waiting batch backup request from slave.
Master HA State to Slot [3]: Realtime backup to slave.
```

The above information indicates the following:

- Slaves 1 is absent, which means that the device is not in use
- The master is waiting for the batch backup request from slave 2
- Slaves 3 is performing real time backup

Table 21-4 display switchover state command output description for the master

Field	Description
Master HA State to Slot *slot-id*	Indicates that this output information is generated by the master. Describes the master/slave switchover states between the master and the slave whose *slot-id* represents its member ID.
Data smooth	The master and the slave are smoothing data.

Display the master/slave switchover state of slave 3.

```
<Sysname> display switchover state slot 3
Slave HA State: Receiving realtime data.
```

The above information indicates that slave 3 is receiving real time backup data.

Table 21-5 display switchover state command output description for a slave

Field	Description
Slave HA State	Indicates that this output information is generated by a slave. Describes the master/slave switchover state of the slave.
Waiting	The slave is ready, and is waiting to enter the batch backup state.

irf auto-update enable

Syntax

irf auto-update enable

undo irf auto-update enable

View

System view

Default Level

3: Manage level

Parameters

None

Description

Use the **irf auto-update enable** command to enable the auto update of boot files in an IRF.

Use the **undo irf auto-update enable** command to disable this function.

This function is enabled by default.

Note the following:

- Before adding a device into an IRF, ensure that the device and the IRF master have the same software version
- After loading the master's boot file automatically, a slave configures the file as the boot file for the next boot and reboots automatically.
- Because system boot file occupies large memory space, to make the auto upgrade succeed, ensure that there is enough space on the storage media of the slave.
- If the downloaded boot file and the local file have duplicate filenames, the local file is overwritten. To avoid this, check the names of local files and make sure whether you need to save the one with the same filename or back it up before downloading the boot file.

Examples

Enable auto upgrade of boot files in an IRF.

```
<Sysname> system-view
[Sysname] irf auto-update enable
```

irf link-delay

Syntax

irf link-delay *interval*

undo irf link-delay

View

System view

Default Level

3: Manage level

Parameters

Interval: Time interval in milliseconds for the link layer to report a link-down event of an IRF, in the range 200 to 2000.

Description

Use the **irf link-delay** command to set the delay time for the link layer to report a link-down state event of an IRF.

Use the **undo irf link-delay** command to restore the default.

This function is disabled by default.

Examples

Set the delay time for the link layer to report a link-down event of the current IRF to 300 milliseconds.

```
<Sysname> system-view
```

```
[Sysname] irf link-delay 300
```

irf mac-address persistent

Syntax

irf mac-address persistent { **timer** | **always** }

undo irf mac-address persistent

View

System view

Default Level

3: Manage level

Parameters

timer: IRF bridge MAC address preservation mode, with this keyword, the IRF bridge MAC address will be preserved for 6 minutes after the master leaves.

always: IRF bridge MAC address preservation mode, with this keyword, the IRF bridge MAC address will be preserved permanently.

Description

Use the **irf mac-address persistent** command to configure the preservation time of IRF bridge MAC address.

Use the **undo irf mac-address persistent** command to configure the IRF not to preserve the IRF bridge MAC address as soon as the master leaves.

By default, IRF bridge MAC address is preserved for 6 minutes.

- Preserve for six minutes: After the master leaves, the bridge MAC address will not change within six minutes. If the master does not come back after six minutes, the IRF system will use the bridge MAC address of the newly elected master as that of the IRF.
- Preserve permanently: No matter the master leaves the IRF or not, the IRF bridge MAC address remains unchanged.
- Not preserved: As soon as the master leaves, the system will use the bridge MAC address of the newly elected master as that of the IRF.

Examples

Configure the IRF bridge MAC address to be preserved permanently.

```
<Sysname> system-view
[Sysname] irf mac-address persistent always
```

irf member irf-port

Syntax

irf member *member-id* **irf-port** *irf-port-id* **port** *port-list*

undo irf member *member-id* **irf-port** *irf-port-id*

View

System view

Default Level

3: Manage level

Parameters

member-id: ID of the IRF member, in the range 1 to 4. With this argument, you can configure the IRF ports of another IRF member on this device. You can view the member IDs of in IRF by using the **display irf** command.

irf-port-id: ID of an enabled IRF port, the value can be either 1 (the left port) or 2 (the right port).

port-list: Physical IRF port list. The *port-list* is in the format of { *port* }&<1-4>, where

- *port* indicates the port ID. The physical IRF ports are numbered according to their physical locations on the rear panel of the Switch 4210G series. With the rear panel facing you, the physical IRF ports are numbered successively from left to right: ports on the interface module in slot 1 are numbered 1 and 2, and ports on the interface module in slot 2 are numbered 3 and 4.
- &<1-4> indicates that you can specify one to four ports at one time. When multiple ports are specified, they aggregate together to form an IRF port. On the Switch 4210G series, only the physical IRF ports that are on the same interface module can be aggregated together.

Note

For the correspondence between an IRF port and physical IRF port, refer to the related part in *IRF Configuration*.

Description

Use the **irf member irf-port** command to bind the physical IRF port(s) to an IRF port of a device, and enable IRF on the IRF port simultaneously.

Use the **undo irf member irf-port** command to disable IRF on an IRF port. If this IRF port is aggregated from multiple physical IRF ports, the aggregated physical ports are disaggregated.

Note the following:

- The above configuration takes effect after the reboot of the device.
- An IRF port should be enabled first before it can connect to other devices to form an IRF.

Examples

Bind physical IRF port 1 to IRF port 1, and enable IRF port 1 of the local device.

```
<Sysname> system-view
[Sysname] irf member 1 irf-port 1 port 1
```

Bind physical IRF ports 3 and 4 to IRF port 2 of member 3, and enable IRF on the IRF port.

```
<Sysname> system-view
[Sysname] irf member 3 irf-port 2 port 3 4
```

irf member priority

Syntax

irf member *member-id* **priority** *priority*

undo irf member *member-id* **priority**

View

System view

Default Level

3: Manage level

Parameters

member-id: ID of the IRF member, in the range 1 to 4. With this argument, you can specify a priority for another IRF member on this device. You can view the member IDs and current priorities of IRF members by using the **display irf** command.

priority: Priority value, in the range 1 to 32.

Description

Use the **irf member priority** command to specify a priority for an IRF member.

Use the **undo irf member priority** command to restore the default.

By default, the priority of an IRF member is 1.

The greater the priority value, the higher the priority. A member with a higher priority is more likely to be a master, and more likely to preserve its ID in a member ID collision.

Note the following:

- You can specify a priority for a member of the current IRF only.
- The setting of priority takes effect right after your configuration.

Examples

Specify a priority for the local device.

```
<Sysname> display irf
Switch     Role        Priority      CPU-MAC
    1      Slave       13            000f-e2b8-1f84
    2      Slave       1             000f-e220-2122
   *3      Master      20            000f-e2b8-1a82
   +4      SlaveWait   1             000f-e2c8-1b82
-------------------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.
The Bridge MAC of the IRF is : 000f-e2b8-1a67
Auto upgrade               : yes
Mac persistent             : 6 min
```

The above information indicates that the member ID of the local device is 4, and you can specify a priority for the local device by providing its member ID.

```
<Sysname> system-view
```

```
[Sysname] irf member 4 priority 16
```

Specify a priority for member 2 in the current IRF.

```
<Sysname> system-view
[Sysname] irf member 2 priotiry 32
```

irf member renumber

Syntax

irf member *member-id* **renumber** *new-member-id*

undo irf member *member-id* **renumber**

View

System view

Default Level

3: Manage level

Parameters

member-id: ID of the IRF member, in the range 1 to 4. With this argument, you can modify a member ID of another IRF member on this device. You can view the member IDs of in an IRF by using the **display irf** command.

new-member-id: New ID of the IRF member, in the range 1 to 4.

Description

Use the **irf member renumber** command to set a member ID for a device.

Use the **undo irf member renumber** command to cancel the configuration.

By default, the member ID of an IRF member is 1.

Note the following:

- The above setting takes effect after the reboot of the device.
- In an IRF, member IDs are not only used to identify devices, but also used to identify the port configurations on different member devices in the configuration file. Therefore, modifying a member ID may cause device configuration changes or even losses, so modify member ID with caution. For example, three members (of same device model) with the member IDs of 1, 2 and 3 are connected to an IRF port. Suppose that each member has several ports: change the member ID of device 2 to 3, change that of device 3 to 2, reboot both devices, and add them into the IRF again. Then device 2 will use the original port configurations of device 3, and device 3 will use those of device 2.
- When the newly added device and another member have duplicated member IDs, the existing member can preserve its ID, and the system will automatically assign the smallest unused member ID to the new member.

Examples

Set the member ID of the local device (the current member ID is 1) to 3.

```
<Sysname> system-view
[Sysname] irf member 1 renumber 3
```

```
Warning: Renumbering the switch number may result in configuration change or loss.
Continue?[Y/N]:Y
```

irf switch-to

Syntax

irf switch-to *member-id*

View

User view

Default Level

3: Manage level

Parameters

member-id: ID of the IRF member. The *member-id* argument in this command cannot be the member ID of the master. You can view the member IDs of in an IRF by using the **display irf** command.

Description

Use the **irf switch-to** command to redirect to the specified slave device, so that you can access the slave device directly.

When you access an IRF, you actually log in to the master device. The console of the master is displayed as the operation interface of the access terminal. After you execute this command, you are redirected to the specified slave device, which is equal to log in to the salve directly. The operation interface of the access terminal switches from the console of the master to that of the slave, and the system enters the user view of the slave. You will see that the command prompt changes to the following format: <Sysname-*member ID*>, for example, <Sysname-2>.

After this command is executed, the instructions that you input at the terminal will be forwarded to the specified slave, without being processed by the local device. Currently, you can execute the following commands on a slave:

- **display**
- **quit**
- **return**
- **system-view**
- **debugging**
- **terminal debugging**
- **terminal trapping**
- **terminal logging**

The console of the master will not time out and will not output any information. You can return to the console of the master by pressing the **Ctrl+K** keys, or execute the **quit** or **return** command. The master is therefore reactivated and is ready for outputting information.

Examples

Redirect to member 2.

```
<Sysname> irf switch-to 2
<Sysname-Slave#2>
```

22 IPC Configuration Commands

- The **display** commands in this document display information of active nodes only.
- For a centralized device, “local node” refers to a local device; for a distributed device, “local node” refers to the active main control board.

IPC Configuration Commands

display ipc channel

Syntax

display ipc channel { **node** *node-id* | **self-node** }

View

Any view

Default Level

1: Monitor level

Parameters

node *node-id*: Displays channel information of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

self-node: Displays the channel information of the local node.

Description

Use the **display ipc channel** command to display the channel information of the specified node.

Examples

Display channel information of node **6**.

```
<Sysname> display ipc channel node 6
ChannelID     Description
---------------------------------------------
14            Prehistorical channel, NO.2
15            Prehistorical channel, NO.6
16            Prehistorical channel, NO.7
19            Prehistorical channel, NO.1
25            Prehistorical channel, NO.4
```

```
26            Prehistorical channel, NO.8
27            FIB4
32            Prehistorical channel, NO.3
33            Prehistorical channel, NO.11
34            Prehistorical channel, NO.9
35            IPC test channel
37            Prehistorical channel, NO.12
43            Prehistorical channel, NO.14
45            Prehistorical channel, NO.5
53            Prehistorical channel, NO.13
62            Prehistorical channel, NO.10
```

Table 22-1 display ipc channel command output description

Field	Description
ChannelID	Channel number, which has been predefined and assigned by the system. One channel number corresponds to one module. The **display ipc channel** command displays the numbers of the current active modules.
Description	Description information, which is generated by the internal software of the device, is used to describe the functions of a channel. For example, “FIB4” indicates that the channel is used for Layer 3 fast forwarding; “Prehistorical channel, NO.2” indicates that no description is defined for the channel, and the channel is the second channel established.

display ipc link

Syntax

display ipc link { **node** *node-id* | **self-node** }

View

Any view

Default Level

1: Monitor level

Parameters

node *node-id*: Displays the link information of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

self-node: Displays the link status information of the local node.

Description

Use the **display ipc link** command to display the link status information of the specified node.

Examples

Display link status information of the local node.

```
<Sysname> display ipc link self-node
Dst-NodeID       LinkStatus
-----------------------------------------
```

```
1                UP
2                DOWN
```

The above prompt information indicates that:

- A connection exists between the local node and node 1, and the connection is up;
- A connection exists between the local node and node 2, and the connection is down.

Table 22-2 display ipc link command output description

Field	Description
Dst-NodeID	Number of the peer node
LinkStatus	Link status, which may take the following values: UP: A connection is established. DOWN: A connection is terminated.

display ipc multicast-group

Syntax

display ipc multicast-group { **node** *node-id* | **self-node** }

View

Any view

Default Level

1: Monitor level

Parameters

node *node-id*: Displays the multicast group information of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

self-node: Displays the multicast group information of the local node.

Description

Use the **display ipc multicast-group** command to display the multicast group information of the specified node.

Examples

Display the multicast group information of node **6**.

```
<Sysname> display ipc multicast-group node 6
GroupID    Status    ChannelID
---------------------------------
8          INUSE     12
```

Table 22-3 display ipc group command output description

Field	Description
GroupID	Multicast group ID
Status	Link status, which may take the following values: INUSE: The multicast group is in use. DELETE: The multicast group is to be deleted.
ChannelID	Channel number

display ipc node

Syntax

display ipc node

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display ipc node** command to display node information.

Examples

Display node information of the device.

```
<Sysname> display ipc node
Self node ID: 6
Current active node ID: 2,3,6,8
```

Table 22-4 display ipc node command output description

Field	Description
Self node ID	Number of the local node
Current active node ID	List of the current active nodes

display ipc packet

Syntax

display ipc packet { **node** *node-id* | **self-node** }

View

Any view

Default Level

1: Monitor level

Parameters

node *node-id*: Displays the packet statistics information of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

self-node: Displays the packet statistics information of the local node.

Description

Use the **display ipc packet** command to display the packet statistics information of the specified node.

Examples

Display the packet statistics information of the local node.

```
<Sysname> display ipc packet self-node
ChannelID Sent-fragments Sent-packets Received-fragments Received-packets
------------------------------------------------------------------------------
11        828            810          819               810
13        0              0            0                 0
14        5              3            5                 5
15        0              0            0                 0
16        0              0            0                 0
17        50             50           37                35
19        0              0            0                 0
```

Table 22-5 display ipc packet command output description

Field	Description
ChannelID	Channel number
Sent-fragments	Number of fragments sent
Sent-packets	Number of packets sent (whether a packet is fragmented depends on the interface MTU. If the number of bytes the packet is larger than the MTU, the packet is fragmented; if smaller than or equal to the MTU, the packet is sent.)
Received-fragments	Number of fragments successfully received
Received-packets	Number of packets successfully received (if fragments are received on an interface, the system reassembles the fragments and sends a complete packet to the upper layer software.)

display ipc performance

Syntax

display ipc performance { **node** *node-id* | **self-node** } [**channel** *channel-id*]

View

Any view

Default Level

1: Monitor level

Parameters

node *node-id*: Displays the IPC performance statistics information of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

self-node: Displays the IPC performance statistics information of the local node.

channel *channel-id*: Displays the IPC performance statistics information of the specified channel, where *channel-id* represents the channel number, in the range of 0 to 159.

Description

Use the **display ipc performance** command to display IPC performance statistics information.

If IPC performance statistics is enabled, the command displays the current IPC performance statistics; if IPC performance statistics is disabled, the command displays the IPC performance statistics at the time when IPC performance statistics is disabled.

Related commands: **ipc performance enable**.

Examples

Display IPC performance statistics information of node **6**.

```
<Sysname> display ipc performance node 6
Peak: Peak rate (pps)
10Sec: Average rate in the last 10 seconds (pps)
1Min: Average rate in the last 1  minute (pps)
5Min: Average rate in the last 5  minutes (pps)
Total-Data: Total number of data (packets)

Statistics for packets sent successfully:
Peak       10Sec        1Min       5Min       Total-Data
------------------------------------------------------------
1          1            1          0          80
Statistics for packets recieved successfully:
Peak       10Sec        1Min       5Min       Total-Data
------------------------------------------------------------
1          1            1          0          82
Statistics for packets acknowledged:
Peak       10Sec        1Min       5Min       Total-Data
------------------------------------------------------------
1          1            1          0          78
```

Table 22-6 display ipc performance command output description

Field	Description
Peak	Peak rate (average rate is counted every 10 seconds, the greatest value of which is taken as the peak rate), in pps
10Sec	Average rate in the past 10 seconds, in pps
1Min	Average rate in the past 1 minute, in pps

Field	Description
5Min	Average rate in the past 5 minutes, in pps
Total-Data	Total amount of data collected from the time when IPC performance statistics was enabled to the time when this command is executed

display ipc queue

Syntax

display ipc queue { **node** *node-id* | **self-node** }

View

Any view

Default Level

1: Monitor level

Parameters

node *node-id*: Displays the sending queue information of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

self-node: Displays the sending queue information of the local node.

Description

Use the **display ipc queue** command to display the sending queue information of the specified node.

Examples

Display the sending queue information of the local node.

```
<Sysname> display ipc queue self-node
QueueType  QueueID Dst-NodeID   Length  FullTimes   Packet
-------------------------------------------------------------
UNICAST    0       0           4096    0           0
UNICAST    1       0           4096    0           0
UNICAST    2       0           4096    0           0
UNICAST    3       0           4096    0           0
UNICAST    0       1           4096    0           0
UNICAST    1       1           4096    0           0
UNICAST    2       1           4096    0           0
UNICAST    3       1           4096    0           0
MULTICAST  0       --          4096    0           0
MULTICAST  1       --          4096    0           0
MULTICAST  2       --          512     0           0
MULTICAST  3       --          512     0           0
MULTICAST  4       --          512     0           0
MULTICAST  5       --          512     0           0
MIXCAST    0       --          2048    0           0
MIXCAST    1       --          2048    0           0
```

Table 22-7 display ipc queue command output description

Field	Description
QueueType	Queue type, including: UNICAST: unicast queue MULTICAST: multicast (including broadcast) queue MIXCAST: mixcast queue, which can accommodate unicasts, multicasts and broadcasts
QueueID	Queue number
Dst-NodeID	Peer node number. If no peer node exists, the field is displayed as “--”.
Length	Queue length (namely, number of packets that can be cached)
FullTimes	Times that the queue is full
Packet	Total number of packets in the queue

ipc performance enable

Syntax

ipc performance enable { **node** *node-id* | **self-node** } [**channel** *channel-id*]

undo ipc performance enable [**node** *node-id* | **self-node**] [**channel** *channel-id*]

View

User view

Default Level

1: Monitor level

Parameters

node *node-id*: Enables IPC performance statistics of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

self-node: Enables IPC performance statistics of the local node.

channel *channel-id*: Enables IPC performance statistics information of the specified channel, where *channel-id* represents the channel number, in the range of 0 to 159.

Description

Use the **ipc performance enable** command to enable IPC performance statistics. Use the **undo ipc performance** command to disable IPC performance statistics.

By default, IPC performance statistics is disabled.

When IPC performance statistics is disabled, the statistics data does not change. In this case, if you execute the **display ipc performance** command, the statistics data at the time when ICP performance statistics was disabled.

Examples

Enable IPC performance statistics of node **6** on channel **18**.

```
<Sysname> ipc performance enable node 6 channel 18
```

reset ipc performance

Syntax

reset ipc performance [**node** *node-id* | **self-node**] [**channel** *channel-id*]

View

User view

Default Level

1: Monitor level

Parameters

node *node-id*: Clears the IPC performance statistics information of the specified node, where *node-id* represents the number of the specified node, in the range of 0 to 9.

self-node: Clears the IPC performance statistics information of the local node.

channel *channel-id*: Clears the IPC performance statistics information of the specified channel, where *channel-id* represents the channel number, in the range of 0 to 159.

Description

Use the **reset ipc performance** command to clear IPC performance statistics information.

After this command is executed, the corresponding statistics information will be cleared.

Examples

Clear IPC performance statistics information of node **6** on channel **18**.

```
<Sysname> reset ipc performance node 6 channel 18
```

23 PoE Configuration Commands

PoE Configuration Commands

apply poe-profile

Syntax

apply poe-profile { **index** *index* | **name** *profile-name* }

undo apply poe-profile { **index** *index* | **name** *profile-name* }

View

PoE interface view

Default Level

2: System level

Parameters

index *index*: Index number of the PoE configuration file, in the range 1 to 100.

name *profile-name*: Name of the PoE configuration file, a string of 1 to 15 characters.

Description

Use the **apply poe-profile** command to apply the PoE configuration file to the current PoE interface.

Use the **undo apply poe-profile** command to remove the application of the PoE configuration file to the current PoE interface.

Note that the index number, instead of the name, of the PoE configuration file is displayed when you execute the **display this** command.

Related commands: **display poe-profile**, **apply poe-profile interface**.

Examples

Apply the PoE configuration file named **A20** to the PoE interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name A20
[Sysname-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode route
 apply poe-profile index 1
#
```

apply poe-profile interface

Syntax

apply poe-profile { **index** *index* | **name** *profile-name* } **interface** *interface-range*

undo apply poe-profile { **index** *index* | **name** *profile-name* } **interface** *interface-range*

View

System view

Default Level

2: System level

Parameters

index *index*: Index number of the PoE configuration file, in the range 1 to 100.

name *profile-name*: Name of the PoE configuration file, a string of 1 to 15 characters.

interface-range: Range of Ethernet interface numbers, indicating multiple Ethernet interfaces. The expression is *interface-range* = *interface-type interface-number* [**to** *interface-type interface-number*], where *interface-type interface-number* represents the interface type and interface number. The start interface number should be smaller than the end interface number. Ethernet interface numbers can be in any range. If any interface in the specified range does not support PoE, it is ignored when the PoE configuration file is applied.

Description

Use the **apply poe-profile interface** command to apply the PoE configuration file to one or more PoE interfaces.

Use the **undo apply poe-profile interface** command to remove the application of the PoE configuration file to the specified PoE interface(s).

Related commands: **display poe-profile interface**, **apply poe-profile**.

Examples

Apply the PoE configuration file named ABC to the PoE interface GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] apply poe-profile name ABC interface gigabitethernet 1/0/1
```

Apply the indexed PoE configuration file to PoE interfaces GigabitEthernet 1/0/2 through GigabitEthernet 1/0/8.

```
<Sysname> system-view
[Sysname] apply poe-profile index 5 interface gigabitethernet 1/0/2 to gigabitethernet 1/0/8
```

display poe device

Syntax

display poe device

View

Any view

Default Level

1: Monitor level

Parameters

None

Description

Use the **display poe device** command to display the mapping between ID, module, and member ID of all the power sourcing equipments (PSEs).

Examples

Display the mapping between ID, module, and member ID of each PSE.

```
<Sysname> display poe device
 PSE ID  SlotNo SubSNo PortNum  MaxPower(W)  State   Model
 5       4      0      24       370          on      LSP1POEA
 6       5      0      16       370          on      LSP1POEA
```

Table 23-1 display poe device command output description

Field	Description
PSE ID	ID of the PSE
SlotNo	Member ID number of the PSE
SubSNo	SubSlot number of the PSE
PortNum	Number of PoE interfaces on the PSE
MaxPower(W)	Maximum power of the PSE (W)
State	PSE state: on: The PSE is supplying power. off: The PSE stops supplying power. faulty: The PSE fails.
Model	PSE model

display poe interface

Syntax

display poe interface [*interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Description

Use the **display poe interface** command to display the power information of the specified interface.

If no interface is specified, the power information of all PoE interfaces is displayed.

Examples

Display the power state of GigabitEthernet 1/0/1.

```
<Sysname> display poe interface gigabitethernet 1/0/1
 Port Power Enabled             : enable
 Port Power Priority            : critical
 Port Operating Status          : on
 Port IEEE Class                : 1
 Port Detection Status          : delivering-power
 Port Power Mode                : signal
 Port Current Power             : 11592    mW
 Port Average Power             : 11610    mW
 Port Peak Power                : 11684    mW
 Port Max Power                 : 15400    mW
 Port Current                   : 244      mA
 Port Voltage                   : 51.7     V
 Port PD Description            : IP Phone For Room 101
```

Table 23-2 display poe interface ethernet command output description

Field	Description
Port Power Enabled	PoE state: enabled/disabled • enable: PoE is enabled. • disable: PoE is disabled.
Port Power Priority	Power priority of the PoE interface: • critical (highest) • high • low
Port Operating Status	Operating state of a PoE interface: • off: PoE is disabled. • on: Power is supplied for a PoE interface normally. • power lack: The guaranteed remaining power of the PSE is not high enough to supply power for a critical PoE interface. • power-deny: The PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power. • power-itself: The external equipment is supplying power for itself. • power-limit: The PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power. Port operating status varies with devices.
Port IEEE class	PD power class: 0, 1, 2, 3, 4, and - - indicates not supported.

Field	Description
Port Detection Status	Power detection state of a PoE interface: • disabled: The PoE function is disabled. • searching: The PoE interface is searching for the PD. • delivering-power: The PoE interface is supplying power for the PD. • fault: There is a fault defined in 802.3af. • test: The PoE interface is under test. • other-fault: There is a fault other than defined in 802.3af. • pd-disconnect: The PD is disconnected. Port detection status varies with devices.
Port Power Mode	Power mode of a PoE interface: • signal: Power is supplied over signal cables. • spare: Power is supplied over spare cables. Switch 4210G only support for signal mode.
Port Current Power	Current power of a PoE interface, including PD consumption power and transmission loss The transmission loss usually does not exceed one watt. The specific loss varies with devices.
Port Average Power	Average power of a PoE interface
Port Peak Power	Peak power of a PoE interface
Port Max Power	Maximum power of a PoE interface
Port Current	Current of a PoE interface
Port Voltage	Voltage of a PoE interface
Port PD Description	Description of the PD connected to the PoE interface, which is used to identify the type and location of the PD.

Display the state of all PoE interfaces.

```
<Sysname> display poe interface
 Interface  Enable   Priority  CurPower  Operating   IEEE   Detection
                               (W)       Status      class  Status
 GE1/0/1      enable   low       4.4       on          1      delivering-power
 GE1/0/2      enable   critical  0         on          -      disabled
 GE1/0/3      enable   low       0         on          -      disabled
 GE1/0/4      enable   critical  0         on          -      searching
 GE1/0/5      enable   low       4.0       on          2      delivering-power
 GE1/0/6      enable   low       0         on          -      disabled
 GE1/0/7      disable  low       0         off         -      fault
 GE1/0/8      disable  low       0         off         -      disabled
 GE1/0/9      disable  low       0         off         -      disabled
 GE1/0/10     disable  low       0         off         -      disabled
 GE1/0/11     disable  low       0         off         -      disabled
 GE1/0/12     disable  low       0         off         -      disabled

 ---  2 port(s) on,    8.4(W) consumed,   361.6(W) Remaining ---
```

Table 23-3 display poe interface command output description

Field	Description
Interface	Shortened form of a PoE interface
Enable	PoE state: enabled/disabled • enable: PoE is enabled. • disable: PoE is disabled.
Priority	Power priority of a PoE interface: • critical (highest) • high • low
CurPower	Current power of a PoE interface
Operating Status	Operating state of a PoE interface • off: PoE is disabled. • on: Power is supplied for a PoE interface normally. • power lack: The guaranteed remaining power of the PSE is not high enough to supply power for a critical PoE interface. • power-deny: The PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power. • power-itself: The external equipment is supplying power for itself. • power-limit: The PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power. Port operation status varies with devices.
IEEE class	PD power class defined by IEEE
Detection Status	Power detection state of a PoE interface: • disabled: The PoE function is disabled. • searching: The PoE interface is searching for the PD. • delivering-power: The PoE interface is supplying power for the PD. • fault: There is a fault defined in 802.3af. • test: The PoE interface is under test. • There is a fault other than defined in 802.3af. • pd-disconnect: The PD is disconnected. Power detection state varies with devices.
port(s) on	Number of PoE interfaces that are supplying power
consumed	Power consumed by the current PoE interface
Remaining	Total remaining power of the system

display poe interface power

Syntax

display poe interface power [*interface-type interface-number*]

View

Any view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Description

Use the **display poe interface power** command to display the power information of a PoE interface(s).

If no interface is specified, the power information of all PoE interfaces will be displayed.

Examples

Display the power information of GigabitEthernet 1/0/1.

```
<Sysname> display poe interface power gigabitethernet 1/0/1
Interface  CurPower PeakPower MaxPower PD Description
           (W)       (W)       (W)
 GE1/0/1    15.0      15.3      15.4     Acess Point on Room 509 for Peter
```

Display the power information of all PoE interfaces.

```
<Sysname> display poe interface power
Interface  CurPower PeakPower MaxPower PD Description
           (W)       (W)       (W)
 GE1/0/25    4.4       4.5       4.6        IP Phone on Room 309 for Peter Smith
 GE1/0/26    4.4       4.5       15.4       IP Phone on Room 409 for Peter Pan
 GE1/0/27    15.0      15.3      15.4      Acess Point on Room 509 for Peter
 GE1/0/28    0         0          0         IP Phone on Room 609 for Peter John
 GE1/0/29    0         0          0         IP Phone on Room 709 for Jack
 GE1/0/30    0         0          0         IP Phone on Room 809 for Alien


---  3 port(s) on,   23.8(W) consumed,   776.2(W) Remaining ---
```

Table 23-4 display poe interface power command output description

Field	Description
Interface	Shortened form of a PoE interface
CurPower	Current power of a PoE interface
PeakPower	Peak power of a PoE interface
MaxPower	Maximum power of a PoE interface
PD Description	Description of the PD connected with a PoE interface When the description contains more than 34 characters, the first 30 characters followed by four dots are displayed.
port(s) on	Number of PoE interfaces that are supplying power
consumed	Power currently consumed by all PoE interfaces
Remaining	Total remaining power of the system

display poe pse

Syntax

display poe pse [*pse-id*]

View

Any view

Default Level

1: Monitor level

Parameters

pse-id: PSE ID. You can use the **display poe device** command to view the mapping between PSE ID and member ID. If you enter a PSE ID, the information of the PSE is displayed. Otherwise, the information of all PSEs on the device is displayed.

Description

Use the **display poe pse** command to display the information of the specified PSE.

Examples

Display the information of PSE 6.

```
<Sysname> display poe pse 6
 PSE ID                          : 6
 PSE Slot No                     : 5
 PSE Model                       : LSBMPOEGV48TP
 PSE Power Enabled               : enable
 PSE Power Preempted             : no
 PSE Power Priority              : low
 PSE Current Power               : 130     W
 PSE Average Power               : 20      W
 PSE Peak Power                  : 240     W
 PSE Max Power                   : 200     W
 PSE Remaining Guaranteed        : 120     W
 PSE CPLD Version                : 100
 PSE Software Version            : 200
 PSE Hardware Version            : 100
 PSE Legacy Detection            : disable
 PSE Utilization-threshold       : 80
 PSE Pd-policy Mode              : disable
 PSE PD Disconnect Detect Mode   : DC
```

Table 23-5 display poe pse command output description

Field	Description
PSE ID	ID of the PSE
PSE Slot No	Member ID number of the PSE
PSE Model	Model of the PSE module

Field	Description
PSE Power Enabled	PoE is enabled for the PSE
PSE Power Preempted	PSE power preempted state • no: The power of the PSE is not preempted. • yes: The power of the PSE is preempted so that it cannot supply power, although PoE is enabled for the PSE
PSE Power Priority	Power priority of the PSE
PSE Current Power	Current power of the PSE
PSE Average Power	Average power of the PSE
PSE Peak Power	Peak power of the PSE
PSE Max Power	Maximum power of the PSE
PSE Remaining Guaranteed	Guaranteed remaining power of the PSE = Maximum power of the PSE– the sum of the maximum power of the critical PoE interfaces of the PSE
PSE CPLD Version	PSE CPLD version
PSE Software Version	PSE software version number
PSE Hardware Version	PSE hardware version number
PSE Legacy Detection	Nonstandard PD detection by the PSE: • enable: Enabled • disable: Disabled
PSE Utilization-threshold	PSE power alarm threshold
PSE Pd-policy Mode	PD power management policy mode
PSE PD Disconnect Detect Mode	PD disconnection detection mode

display poe pse interface

Syntax

display poe pse *pse-id* **interface**

View

Any view

Default Level

1: Monitor level

Parameters

pse *pse-id*: Specifies a PSE ID. You can use the **display poe device** command to view the mapping between PSE ID and member ID.

Description

Use the **display poe pse interface** command to display the state of all PoE interfaces connected to the specified PSE.

Examples

Display the state of all PoE interfaces connected to PSE 1.

```
<Sysname> display poe pse 1 interface
 Interface  Enable   Priority  CurPower  Operating   IEEE   Detection
                               (W)       Status      class  Status
 GE1/0/1      enable   low       4.4       on          1    delivering-power
 GE1/0/2      enable   critical  0         power-lack  -    disabled
 GE1/0/3      enable   low       0         power-deny  -    disabled
 GE1/0/4      enable   critical  0         on          -    searching
 GE1/0/5      enable   low       4.0       power-limit 2    delivering-power
 GE1/0/6      enable   low       0         power-itself -   disabled
 GE1/0/7      disable  low       0         off         -    fault
 GE1/0/8      disable  low       0         off         -    disabled
 GE1/0/9      disable  low       0         off         -    disabled
 GE1/0/10     disable  low       0         off         -    disabled
 GE1/0/11     disable  low       0         off         -    disabled
 GE1/0/12     disable  low       0         off         -    disabled

---  2 port(s) on,    8.4(W) consumed,   171.6(W) Remaining ---
```

Table 23-6 display poe pse interface command output description

Field	Description
Interface	Shortened form of a PoE interface
Enable	PoE enabled/disabled state. For the value, see Table 23-2.
Priority	Priority of a PoE interface. For the value, see Table 23-2.
CurPower	Current power of a PoE interface
Operating	Operating state of a PoE interface. For the value, see Table 23-2.
IEEE	PD power class
Detection	Power detection state of a PoE interface. For the value, see Table 23-2.
port(s) on	Number of PoE interfaces that are supplying power
consumed	Power consumed by PoE interfaces on the PSE
Remaining	Remaining power on the PSE

display poe pse interface power

Syntax

display poe pse *pse-id* **interface power**

View

Any view

Default Level

1: Monitor level

Parameters

pse *pse-id*: Specifies a PSE ID. You can use the **display poe device** command to view the mapping between PSE ID and member ID.

Description

Use the **display poe pse interface power** command to display the power information of PoE interfaces connected with the PSE.

Examples

Display the power information of PoE interfaces connected with PSE 1.

```
<Sysname> display poe pse 1 interface power
Interface  CurPower PeakPower MaxPower PD Description
           (W)      (W)       (W)
 GE1/0/25   4.4       4.5       4.6      IP Phone on Room 309 for Peter Smith
 GE1/0/26   4.4       4.5       15.4     IP Phone on Room 409 for Peter Pan
 GE1/0/27   15.0      15.3      15.4     Acess Point on Room 509 for Peter
 GE1/0/28   0         0         5        IP Phone on Room 609 for Peter John
 GE1/0/29   0         0         4        IP Phone on Room 709 for Jack
 GE1/0/30   0         0         5        IP Phone on Room 809 for Alien

---  3 port(s) on,   23.8(W) consumed,   346.2(W) Remaining ---
```

Table 23-7 display poe pse interface power command output description

Field	Description
Interface	Shortened form of a PoE interface
CurPower	Current power of a PoE interface
PeakPower	Peak power of a PoE interface
MaxPower	Maximum power of a PoE interface
PD Description	Description of the PD connected with a PoE interface. When the description contains more than 34 characters, the first 30 characters followed by four dots are displayed.
port(s) on	Number of PoE interfaces that are supplying power
consumed	Power currently consumed by all PoE interfaces
Remaining	Remaining power on the PSE

display poe-profile

Syntax

display poe-profile [**index** *index* | **name** *profile-name*]

View

Any view

Default Level

1: Monitor level

Parameters

index *index*: Index number of the PoE configuration file, in the range 1 to 100.

name *profile-name*: Name of the PoE configuration file, a string of 1 to 15 characters.

Description

Use the **display poe-profile** command to display all information of the configurations and applications of the PoE configuration file.

If no argument is specified, all information of the configurations and applications of existing PoE configuration files is displayed.

Examples

Display all information of the configurations and applications of the current PoE configuration file.

```
<Sysname> display poe-profile
Poe-profile      Index  ApplyNum  Interface   Configuration
 AA3456789012345  1     3          GE1/0/1       poe enable
                                   GE1/0/2       poe priority critical
                                   GE1/0/3

 poe-profileAA    2     1          GE1/0/24      poe enable
                                                 poe max-power 12300

 poe-profileBB    3     0                        poe enable
                                                 poe priority critical
                                                 poe max-power 15400

 ---  3 poe-profile(s) created, 4 port(s) applied  ---
```

Table 23-8 display poe-profile command output description

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
poe-profile(s) created	Number of PoE configuration files
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

Display all information of the configurations and applications of the PoE configuration file whose index number is 1.

```
<Sysname> display poe-profile index 1
 Poe-profile     Index  ApplyNum  Interface  Configuration
 AA3456789012345 1      2         GE1/0/2      poe enable
                                  GE1/0/24     poe priority critical
                                               poe max-power 12300


 ---  2 port(s) applied  ---
```

Table 23-9 display poe-profile index command output description

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

Display all information of the configurations and applications of the PoE configuration file named **AA**.

```
<Sysname> display poe-profile name AA
 Poe-profile     Index  ApplyNum  Interface  Configuration
 AA              1      2         GE1/0/1     poe enable
                                  GE1/0/2      poe priority critical
                                               poe max-power 12300
---  2 port(s) applied  ---
```

Table 23-10 display poe-profile name command output description

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

display poe-profile interface

Syntax

display poe-profile interface *interface-type interface-number*

View

Any view

Default Level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Description

Use the **display poe-profile interface** command to display all information of the configurations and applications of the PoE configuration file that currently takes effect on the specified PoE interface.

Examples

Display all information of the configurations and applications of the current PoE configuration file applied to GigabitEthernet 1/0/1.

```
<Sysname> display poe-profile interface gigabitethernet 1/0/1
Poe-profile     Index  ApplyNum  Interface  Current Configuration
AA3456789012345 1      2         GE1/0/2     poe enable
                                             poe priority critical
```

Table 23-11 display poe-profile interface command output description

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which the PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Current Configuration	Configurations of the PoE configuration file that currently take effect on a PoE interface

Note

Because not all the configurations of a PoE configuration file can be applied successfully, only the configurations that currently take effect on the interface are displayed.

poe disconnect

Syntax

poe disconnect { **ac | dc** }

undo poe disconnect

View

System view

Default Level

2: System level

Parameters

ac: Specifies the PD disconnection detection mode as **ac**.

dc: Specifies the PD disconnection detection mode as **dc**.

Description

Use the **poe disconnect** command to configure a PD disconnection detection mode.

Use the **undo poe disconnect** command to restore the default.

The default PD disconnection detection mode varies with devices.

Note that change to the PD disconnection detection mode may lead to power-off of some PDs.

Examples

Set the PD disconnection detection mode to **dc**.

```
<Sysname> system-view
[Sysname] poe disconnect dc
```

poe enable

Syntax

poe enable

undo poe enable

View

PoE interface view, PoE-profile file view

Default Level

2: System level

Parameters

None

Description

Use the **poe enable** command to enable PoE on a PoE interface.

Use the **undo poe enable** command to disable PoE on a PoE interface.

By default, PoE is disabled on a PoE interface.

Caution

- If a PoE configuration file is already applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.
- If a PoE configuration file is applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE interface view.

Examples

Enable PoE on a PoE interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe enable
```

Enable PoE on a PoE interface through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe enable
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

poe legacy enable

Syntax

poe legacy enable pse *pse-id*

undo poe legacy enable pse *pse-id*

View

System view

Default Level

2: System level

Parameters

pse *pse-id*: Specifies a PSE ID.

Description

Use the **poe legacy enable** command to enable the PSE to detect nonstandard PDs.

Use the **undo poe legacy enable** command to disable the PSE from detecting nonstandard PDs.

By default, the PSE is disabled from detecting nonstandard PDs.

Examples

Enable PSE 2 to detect nonstandard PDs.

```
<Sysname> system-view
[Sysname] poe legacy enable pse 2
```

poe max-power

Syntax

poe max-power *max-power*

undo poe max-power

View

PoE interface view, PoE-profile file view

Default Level

2: System level

Parameters

max-power: Maximum power in milliwatts allocated to a PoE interface. The range of this argument varies with devices.

Description

Use the **poe max-power** command to configure the maximum power for a PoE interface.

Use the **undo poe max-power** command to restore the default.

By default, the maximum power of the PoE interface is 15,400 milliwatts.

Examples

Set the maximum power of GigabitEthernet 1/0/1 to 12,000 milliwatts.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe max-power 12000
```

Set the maximum power of GigabitEthernet 1/0/1 to 12,000 milliwatts through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe max-power 12000
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

poe mode

Syntax

poe mode signal

undo poe mode

View

PoE interface view, PoE-profile file view

Default Level

2: System level

Parameters

signal: Specifies the PoE mode as **signal** (power over signal cables).

Description

Use the **poe mode** command to configure a PoE mode.

Use the **undo poe mode** command to restore the default.

By default, the PoE mode is **signal** (power over signal cables).

The PSE supplies power for a PoE interface in the following two modes: **signal** and **spare**.

- In the signal mode, lines in Category 3 and 5 twisted pair cables used for transmitting data are also used for supplying DC power.
- In the spare mode, lines in Category 3 and 5 twisted pair cables not in use are used for supplying DC power.
- Switch 4210G only support for signal mode.

Examples

Set the PoE mode to **signal** (power over signal cables).

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe mode signal
```

Set the PoE mode to **signal** (power over signal cables) through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe mode signal
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

poe pd-description

Syntax

poe pd-description *string*

undo poe pd-description

View

PoE interface view

Default Level

2: System level

Parameters

string: Description of the PD connected to a PoE interface, a string of 1 to 80 characters.

Description

Use the **poe pd-description** command to configure a description for the PD connected to a PoE interface.

Use the **undo poe pd-description** command to restore the default.

By default, no description is available for the PD connected to a PoE interface.

Examples

Configure the description for the PD connected to GigabitEthernet 1/0/1 as IP Phone for Room 101.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe pd-description IP Phone For Room 101
```

poe pd-policy priority

Syntax

poe pd-policy priority

undo poe pd-policy priority

View

System view

Default Level

2: System level

Parameters

None

Description

Use the **poe pd-policy priority** command to configure a PD power management priority policy.

Use the **undo poe pd-policy priority** command to remove the PD power management priority policy.

By default, no PD power management priority policy is configured.

Examples

Configure a PD power management priority policy

```
<Sysname> system-view
[Sysname] poe pd-policy priority
```

poe priority

Syntax

poe priority { **critical** | **high** | **low** }

undo poe priority

View

PoE interface view, PoE-profile file view

Default Level

2: System level

Parameters

critical: Sets the power priority of a PoE interface to **critical**. The PoE interface whose power priority level is **critical** works in guaranteed mode, that is, power is first supplied to the PD connected to this critical PoE interface.

high: Sets the power priority of a PoE interface to **high**.

low: Sets the power priority of a PoE interface to **low**.

Description

Use the **poe priority** command to configure a power priority level for a PoE interface.

Use the **undo poe priority** command to restore the default.

By default, the power priority of a PoE interface is **low**.

Note that:

- When the PoE power is insufficient, power is first supplied to PoE interfaces with a higher priority level.
- If a PoE configuration file is already applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.
- If a PoE configuration file is applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE interface view.
- If two PoE interfaces have the same priority level, the PoE interface with a smaller ID has the higher priority level.

Examples

Set the power priority of GigabitEthernet 1/0/1 to **critical**.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe priority critical
```

Set the power priority of GigabitEthernet 1/0/1 to **critical** through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe priority critical
[Sysname-poe-profile-abc-1] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] apply poe-profile name abc
```

poe update

Syntax

poe update { **full** | **refresh** } *filename* **pse** *pse-id*

View

System view

Default Level

2: System level

Parameters

full: Specifies to upgrade the PSE processing software in full mode when the software is unavailable.

refresh: Specifies to upgrade the PSE processing software in refresh mode when the software is available.

filename: Name of the upgrade file, a string of 1 to 64 characters. This file must be under the root directory of the file system of the device. The extension of the upgrade file varies with devices.

pse *pse-id*: Specifies a PSE ID.

Description

Use the **poe update** command to upgrade the PSE processing software online.

Caution

- The **full** mode is used only in the case that anomalies occur when you use the **refresh** mode to upgrade the PSE processing software. Do not use the full mode in other circumstances.
- You can use the **full** mode to upgrade the PSE processing software to restore the PSE firmware when the the PSE processing software is unavailable (it means that none of the PoE commands are executed successfully).

Examples

Upgrade the processing software of PSE 2 online.

```
<Sysname> system-view
[Sysname] poe update refresh 0400_001.S19 pse 2
This command will refresh firmware on the specific PSE(s), Continue? [Y/N]:y
 System is downloading firmware into the hardware. Please wait ..................
.....................................................................................
..................
 Refresh firmware on the specific PSE(s) successfully!
```

poe utilization-threshold

Syntax

poe utilization-threshold *utilization-threshold-value* **pse** *pse-id*

undo poe utilization-threshold pse *pse-id*

View

System view

Default Level

2: System level

Parameters

utilization-threshold-value: Power alarm threshold in percentage, in the range 1 to 99.

pse *pse-id*: Specifies a PSE ID.

Description

Use the **poe utilization-threshold** command to configure a power alarm threshold for the PSE.

Use the **undo poe utilization-threshold** command to restore the default power alarm threshold of the PSE.

By default, the power alarm threshold for the PSE is 80%.

The system sends a Trap message when the percentage of power utilization exceeds the alarm threshold. If the percentage of the power utilization always keeps above the alarm threshold, the system does not send any Trap message. Instead, when the percentage of the power utilization drops below the alarm threshold, the system sends a Trap message again.

Examples

Set the power alarm threshold of PSE 2 to 90%.

```
<Sysname> system-view
[Sysname] poe utilization-threshold 90 pse 2
```

poe-profile

Syntax

poe-profile *profile-name* [*index*]

undo poe-profile { **index** *index* | **name** *profile-name* }

View

System view

Default Level

2: System level

Parameters

profile-name: Name of a PoE configuration file, a string of 1 to 15 characters. A PoE configuration file name begins with a letter (a through z or A through Z) and must not contain reserved keywords such as **undo**, **all**, **name**, **interface**, **user**, **poe**, **disable**, **max-power**, **mode**, **priority** and **enable**.

index: Index number of a PoE configuration file, in the range 1 to 100.

Description

Use the **poe-profile** *profile-name* command to create a PoE configuration file and enter PoE-profile view.

Use the **undo poe-profile** command to delete the specified PoE configuration file.

If no index is specified, the system automatically assigns an index to the PoE configuration file, starting from 1.

Note that if a PoE configuration file is already applied to a PoE interface, you cannot delete it. To delete the file, you must first execute the **undo apply poe-profile** command to remove the application of the PoE configuration file to the PoE interface.

Examples

Create a PoE configuration file, name it **abc**, and specify the index number as **3**.

```
<Sysname> system-view
[Sysname] poe-profile abc 3
```